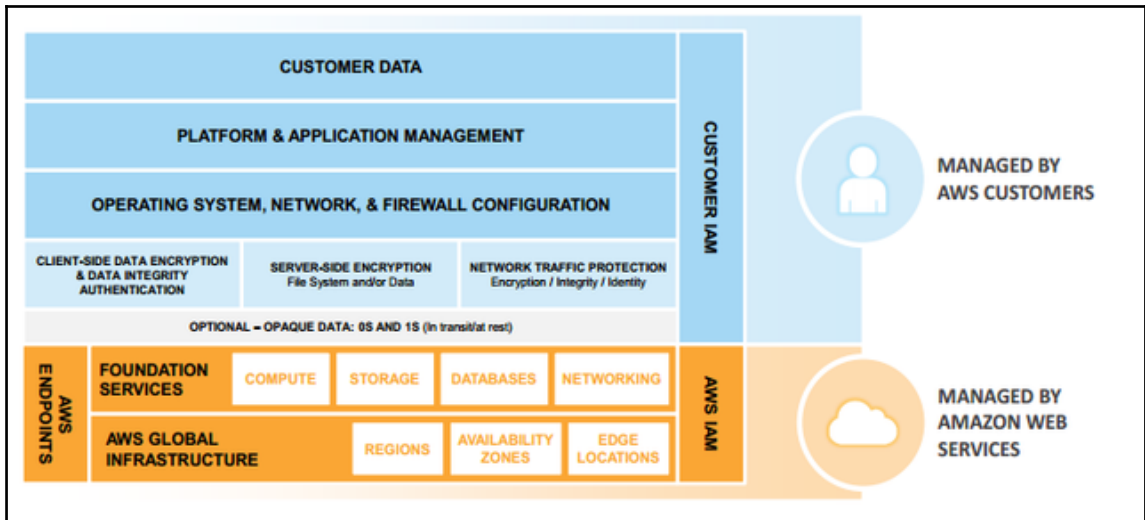
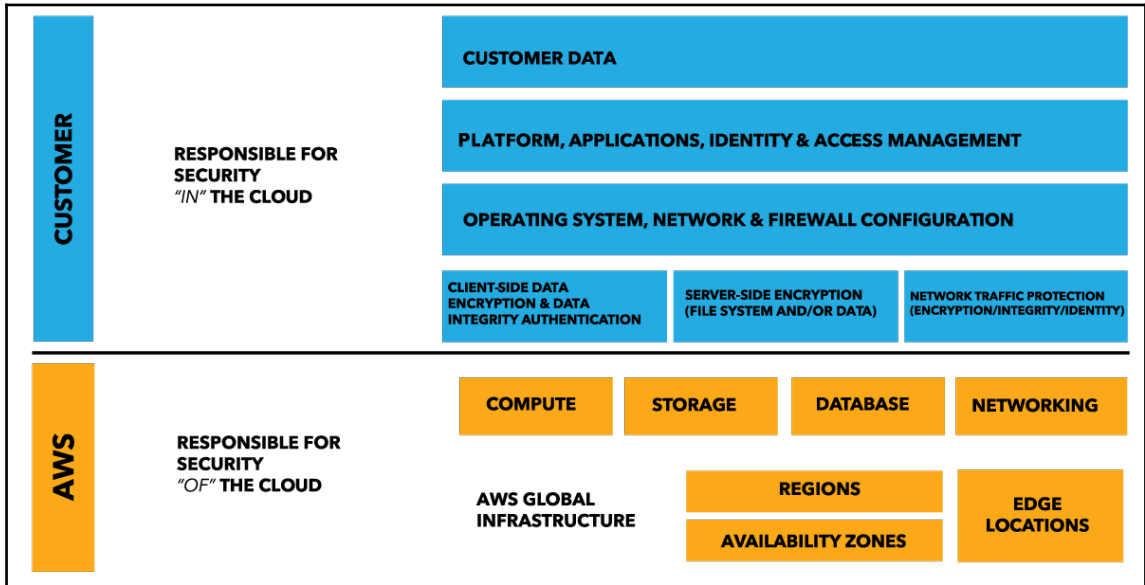
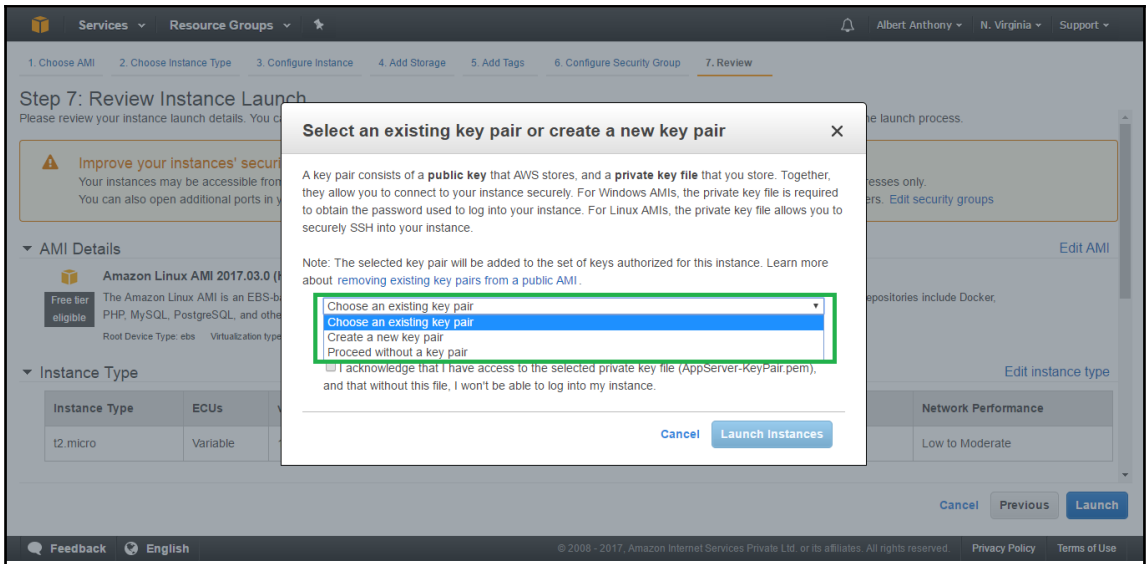


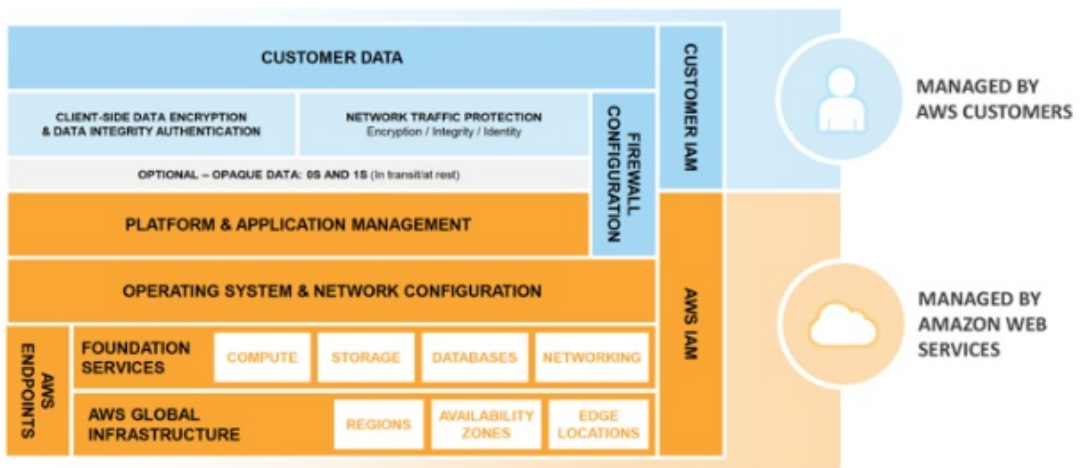
Chapter 1: Overview of Security in AWS



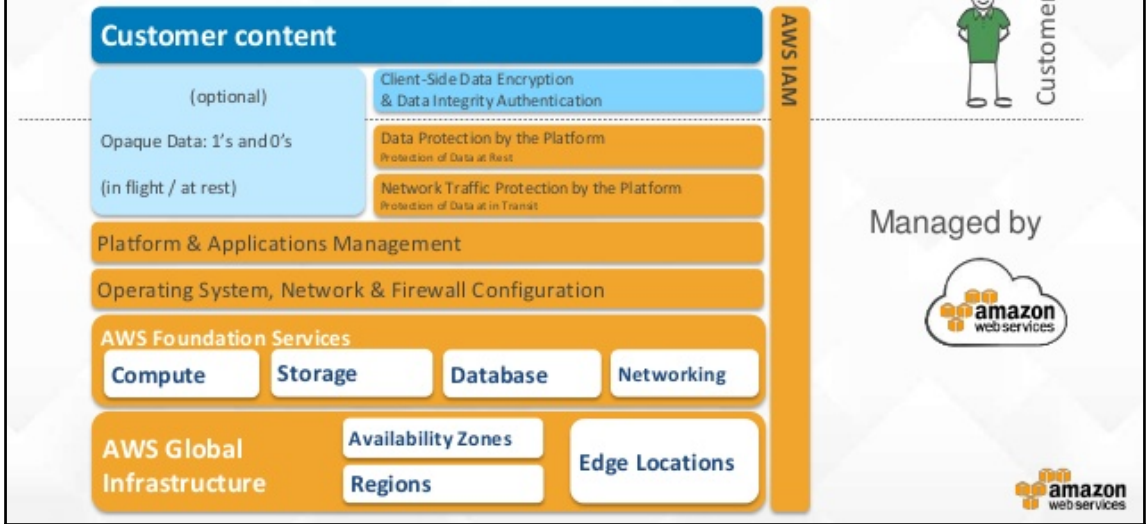


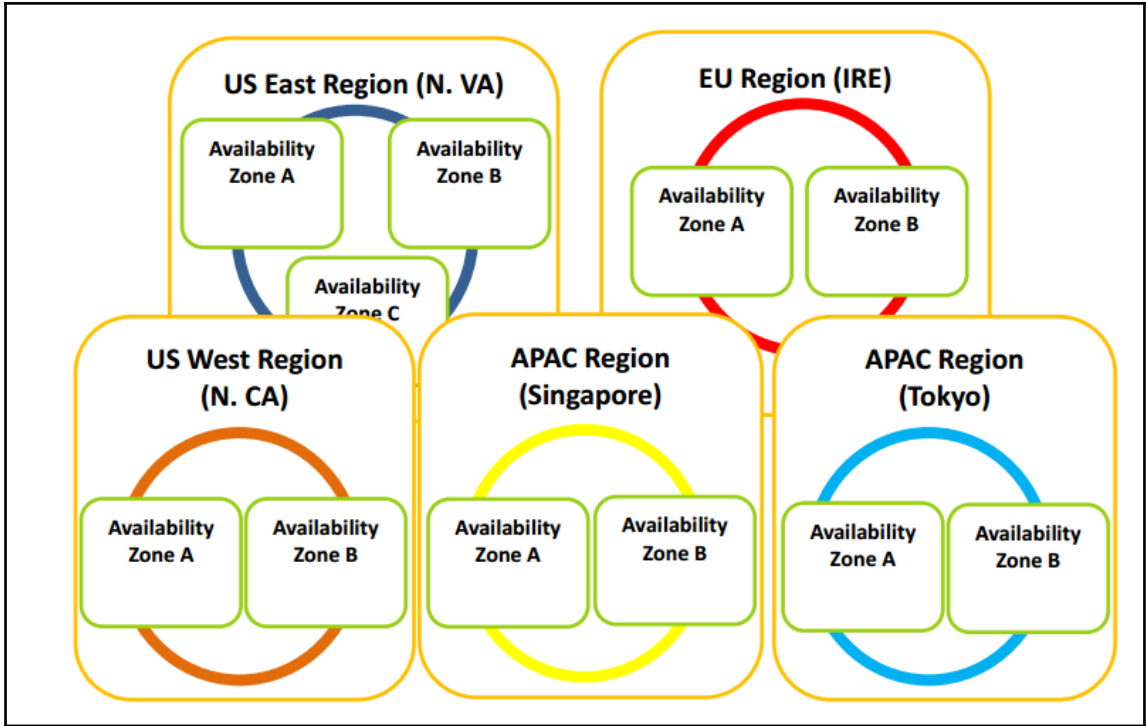
Shared Security Model: Container Services

Such as Amazon RDS and Amazon EMR



AWS Shared Responsibility Model: for Abstract Services







SERVICE HEALTH DASHBOARD

[Amazon Web Services](#) » Service Health Dashboard

Get a personalized view of AWS service health

[Open the Personal Health Dashboard](#)

Current Status - Oct 18, 2017 PDT

Amazon Web Services publishes our most up-to-the-minute information on service availability in the table below. Check back here any time to get current status information, or subscribe to an RSS feed to be notified of interruptions to each individual service. If you are experiencing a real-time, operational issue with one of our services that is not described below, please inform us by clicking on the "Contact Us" link to submit a service issue report. All dates and times are Pacific Time (PST/PDT).

North America	South America	Europe	Asia Pacific	Contact Us
Recent Events		Details		RSS
✓	AWS Direct Connect (Oregon)	[RESOLVED] Network Connectivity	more ▾	
✓	AWS Internet Connectivity (Oregon)	[RESOLVED] Network Connectivity	more ▾	
Remaining Services		Details		RSS
✓	Amazon API Gateway (Montreal)	Service is operating normally		

Customer Responsibility

Customer Data

Platform, Applications, Identify & Access Management

Operating System, Network & Firewall Configuration

Client Side Data Encryption & Data Integrity Authentication

Server Side Encryption (File System and/or Data)

Network Traffic Protection (Encryption/Integrity/Identity)

Trusted Advisor Dashboard



Cost Optimization



0 0 0

Performance



1 0 0

Security



4 0 1

Fault Tolerance



0 0 0

Recommended Actions

Security Groups - Specific Ports Unrestricted

Refreshed: a few seconds ago



Checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports.

11 of 33 security group rules allow unrestricted access to a specific port.

Services ▾ Resource Groups ▾

Albert Anthony ▾ N. Virginia ▾ Support ▾

AWS Config

Rules

Resources

Settings

Rules

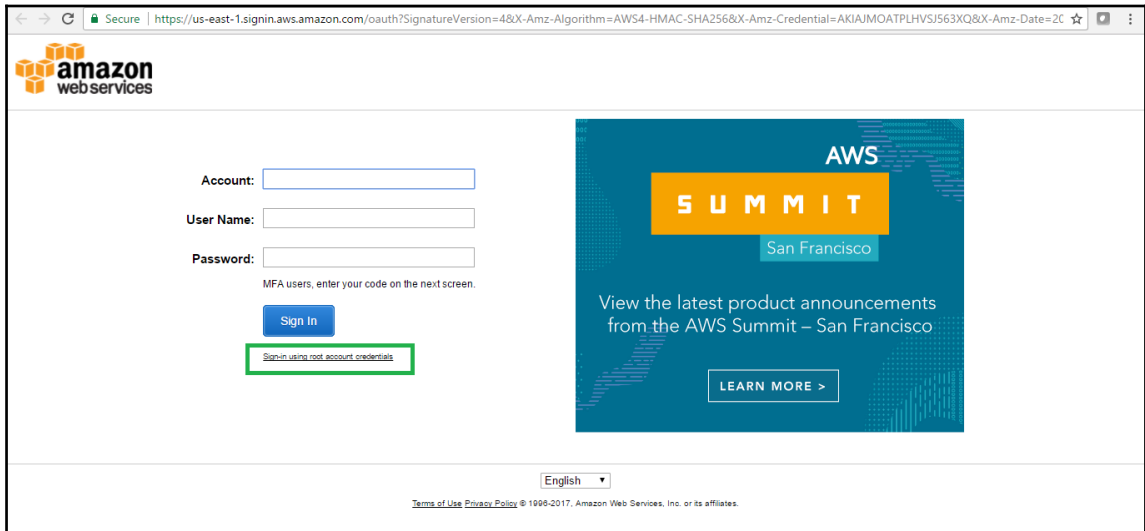
Status ⓘ

Rules represent your desired configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and summarizes the results in the following table.

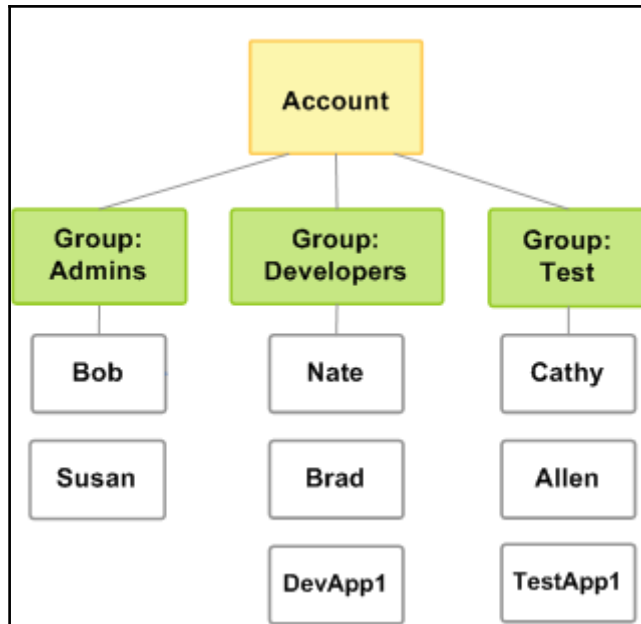
[+ Add rule](#)

Rule name	Compliance	Edit rule
encrypted-volumes	2 noncompliant resource(s)	
iam-password-policy	1 noncompliant resource(s)	
ec2-instances-in-vpc	Compliant	
cloudtrail-enabled	Compliant	
cloudwatch-alarm-settings-check	No results reported	
eip-attached	No resources in scope	

Chapter 2: AWS Identity and Access Management




<input type="checkbox"/>	User name	Groups	Access key age	Password age	Last activity
<input type="checkbox"/>	WVUser1	WVInternational	None	44 days	None
<input type="checkbox"/>	Test-Allen	WVInternational	None	44 days	None
<input type="checkbox"/>	sliamuser	IAM-View-Only-Users	150 days	150 days	130 days
<input type="checkbox"/>	SL-S3-EC2-...	S3-ReadOnly-Users	53 days	None	53 days
<input type="checkbox"/>	SL-IAM-Us...	AdminGroup	45 days	None	39 days
<input type="checkbox"/>	SL-IAM-LAB	None	3 days	3 days	None
<input type="checkbox"/>	SL-CLI-User	None	3 days	None	None




Create role

1 Trust 2 Permissions 3 Review


Select type of trusted entity




AWS service



Another AWS account



Web identity



Saml 2.0 federation

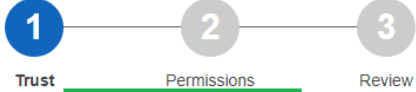
Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose the service that will use this role


API Gateway	Data Pipeline	IoT	Service Catalog
Auto Scaling	Directory Service	Lambda	Storage Gateway
Batch	DynamoDB	Lex	

* Required Cancel **Next: Permissions**


Create role




Trust




AWS service



Another AWS account



Web identity



SAML
Saml 2.0 federation

Allows users that are federated with SAML 2.0 to assume this role to perform actions in your account. [Learn more](#)

Choose a SAML 2.0 provider

If you're creating a role for API access, choose an Attribute and then type a Value to include in the role. This restricts access to users with the specified attributes.

SAML provider [Create new provider](#) | [Refresh](#)

Allow programmatic access only
 Allow programmatic and AWS Management Console access

* Required

Cancel

Next: Permissions

Create role

- 1 Trust
- 2 Permissions
- 3 Review



AWS service



Another AWS account



Web identity

SAML

Saml 2.0 federation

Allows entities in other accounts to perform actions in this account. [Learn more](#)
Specify accounts that can use this role

Account ID*

- Options
- Require external ID (Best practice when a third party will assume this role)
 - Require MFA

* Required

Cancel

Next: Permissions

Create role

- 1 Trust
- 2 Permissions
- 3 Review

Select type of trusted entity



AWS service



Another AWS account



Web identity

SAML

Saml 2.0 federation

Allows users federated by the specified external web identity or OpenID Connect (OIDC) provider to assume this role to perform actions in your account. [Learn more](#)

Choose a web identity provider

Identity provider

[Create new provider](#)

[Refresh](#)

* Required

Cancel

Next: Permissions

Search IAM

IAM Resources

Users: 26 Roles: 44
 Groups: 12 Identity Providers: 0
 Customer Managed Policies: 32

Security Status 5 out of 5 complete.

- Delete your root access keys ▼
- Activate MFA on your root account ▼
- Create individual IAM users ▼
- Use groups to assign permissions ▼

Dashboard
 Groups
 Users
 Roles
 Policies
 Identity providers
 Account settings
 Credential report

Filter: Job function

<input type="checkbox"/>	Policy name ▼	Type	Attachments ▼	Description
<input type="checkbox"/>	▶ AdministratorAccess	Job function	4	Provides full access to AWS services and resources.
<input type="checkbox"/>	▶ Billing	Job function	2	Grants permissions for billing and cost management. This includ
<input type="checkbox"/>	▶ DatabaseAdministrator	Job function	0	Grants full access permissions to AWS services and actions req
<input type="checkbox"/>	▶ DataScientist	Job function	0	Grants permissions to AWS data analytics services.
<input type="checkbox"/>	▶ NetworkAdministrator	Job function	0	Grants full access permissions to AWS services and actions req
<input type="checkbox"/>	▶ PowerUserAccess	Job function	0	Provides full access to AWS services and resources, but does n
<input type="checkbox"/>	▶ SecurityAudit	Job function	0	The security audit template grants access to read security config
<input type="checkbox"/>	▶ SupportUser	Job function	0	This policy grants permissions to troubleshoot and resolve issue

Create Policy

Step 1 : Create Policy
 Step 2 : Set Permissions
 Step 3 : Review Policy

Create Policy

A policy is a document that formally states one or more permissions. Create a policy by copying an AWS Managed Policy, using the Policy Generator, or typing your own custom policy.

Copy an AWS Managed Policy
 Start with an AWS Managed Policy, then customize it to fit your needs. Select

Policy Generator
 Use the policy generator to select services and actions from a list. The policy generator uses your selections to create a policy. Select

Create Your Own Policy
 Use the policy editor to type or paste in your own policy. Select

IAM Policy Simulator

Mode: Existing Policies | Albert Anthony

Policies Back

Selected group: **IAMAdministrator**

IAM Policies

Filter

IAMFullAccess

Resource Policies

Policy Simulator

AWS Identity a... | 2 Action(s) sele... Select All Deselect All Reset Contexts Clear Results Run Simulation

▶ **Global Settings**

Action Settings and Results [5 actions selected, 0 actions not simulated, 2 actions allowed, 3 actions denied.]

Service	Action	Resource Type	Simulation Resource	Permission
▶ Amazon SQS	DeleteMessage	not required	*	denied Implicitly denied (no matchi...
▶ Amazon SQS	AddPermission	not required	*	denied Implicitly denied (no matchi...
▶ Amazon SQS	CreateQueue	not required	*	denied Implicitly denied (no matchi...
▶ AWS Identity and Acces...	CreateGroup	group	*	allowed 1 matching statements.
▶ AWS Identity and Acces...	CreatePolicy	policy	group	allowed 1 matching statements.

Services ▾ Resource Groups ▾ Albert Anthony ▾ Global ▾ Support ▾

Search IAM

Users > Albert

Summary

User ARN am:aws.iam::902891488394:user/Albert
Path /
Creation time 2016-08-25 10:45 UTC+0530

Permissions **Groups (1)** **Security credentials** **Access Advisor**

Access advisor shows the service permissions granted to this user and when those services were last accessed. You can use this information to revise your policies. [Learn more](#)

Note: recent activity usually appears within 4 hours. Access Advisor tracking began on Oct 1, 2015 [Learn more](#)

Filter: No filter ▾ Search Showing 73 results

Service Name	Policies Granting Permissions	Last Accessed
AWS Identity and Access Management	AdministratorAccess	144 days ago
Amazon S3	AdministratorAccess	145 days ago
Amazon EC2	AdministratorAccess	162 days ago
Elastic Load Balancing	AdministratorAccess	314 days ago

Services ▾ Resource Groups ▾

Search IAM

Dashboard
Groups
Users
Roles
Policies
Identity providers
Account settings
Credential report

Encryption keys

▼ Password Policy

A password policy is a set of rules that define the type of password an IAM user can set. For more information about password policies, go to [Managing Passwords](#) in Using IAM.

Modify your existing password policy below.

Minimum password length:

- Require at least one uppercase letter ⓘ
- Require at least one lowercase letter ⓘ
- Require at least one number ⓘ
- Require at least one non-alphanumeric character ⓘ
- Allow users to change their own password ⓘ
- Enable password expiration ⓘ
Password expiration period (in days):
- Prevent password reuse ⓘ
Number of passwords to remember:
- Password expiration requires administrator reset ⓘ

[Apply password policy](#) [Delete password policy](#)

Services ▾ Resource Groups ▾

Albert Anthony ▾ Global ▾ Support ▾

Search IAM

Dashboard
Groups
Users
Roles
Policies
Identity providers
Account settings
Credential report

Encryption keys

Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management, see [AWS Security Credentials in AWS General Reference](#).

To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials in AWS General Reference](#).

- + Password
- + Multi-Factor Authentication (MFA)
- + Access Keys (Access Key ID and Secret Access Key)
- + CloudFront Key Pairs
- + X.509 Certificates
- Account Identifiers

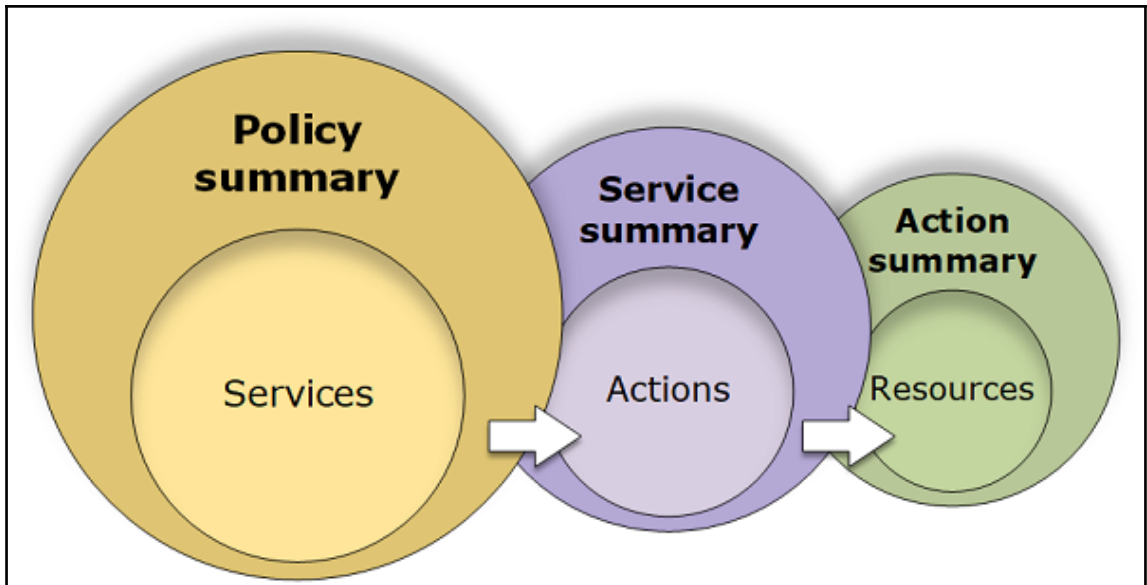
You use your 12-digit account ID to reference your account programmatically and in other contexts. You use your canonical user ID to configure [Amazon S3 access control lists \(ACLs\)](#).

AWS Account ID:

Canonical User ID:

- My Account
- My Organization
- My Billing Dashboard
- My Security Credentials**
- Sign Out

Console



Chapter 3: AWS Virtual Private Cloud

The screenshot shows the AWS VPC Dashboard. The left sidebar contains navigation options for VPC resources. The main area displays the 'Resources' section for a selected VPC, listing various AWS resources. A green box highlights the resource counts. The 'Service Health' section on the right shows the status of Amazon VPC and Amazon EC2 services. Below that, there is an 'Additional Information' section with links to documentation and forums.

Resources

Note: Your Instances will launch in the region.

You are using the following Amazon VPC resources in the region:

2 VPCs	2 Internet Gateways
0 Egress-only Internet Gateways	4 Subnets
4 Route Tables	2 Network ACLs
1 Elastic IP	0 VPC Peering Connections
0 Endpoints	0 Nat Gateways
4 Security Groups	1 Running Instance
0 VPN Connections	0 Virtual Private Gateways
0 Customer Gateways	

Service Health

Current Status	Details
✓ Amazon VPC - Asia Pacific (Mumbai)	Service is operating normally
✓ Amazon EC2 - Asia Pacific (Mumbai)	Service is operating normally

[View complete service health details](#)

Additional Information

- [VPC Documentation](#)
- [All VPC Resources](#)
- [Forums](#)
- [Report an Issue](#)

VPN Connections

Amazon VPC enables you to use your own isolated resources within the AWS cloud, and then connect those resources directly to your own datacenter using industry-standard encrypted IPsec VPN connections.

[Create VPN Connection](#)

The screenshot shows the AWS Route Tables console. The top section displays a list of route tables with columns for Name, Route Table ID, Explicitly Associated, Main, and VPC. A green box highlights the selected route table. Below the list, the 'Routes' tab is active, showing a table of routes with columns for Destination, Target, Status, and Propagated.

Route Tables

Name	Route Table ID	Explicitly Associated	Main	VPC
NAT Route Table	rtb-0b311762	0 Subnets	No	vpc-0466956d Default VPC
Custom Route Table	rtb-063e186f	1 Subnet	No	vpc-3cd49d55 My-Lab-VPC
	rtb-9e50a2f7	0 Subnets	Yes	vpc-0466956d Default VPC
	rtb-59331530	1 Subnet	Yes	vpc-3cd49d55 My-Lab-VPC

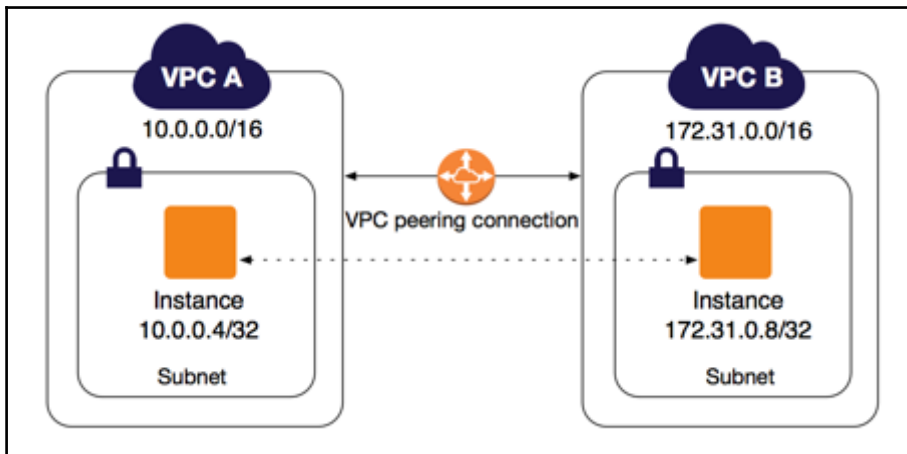
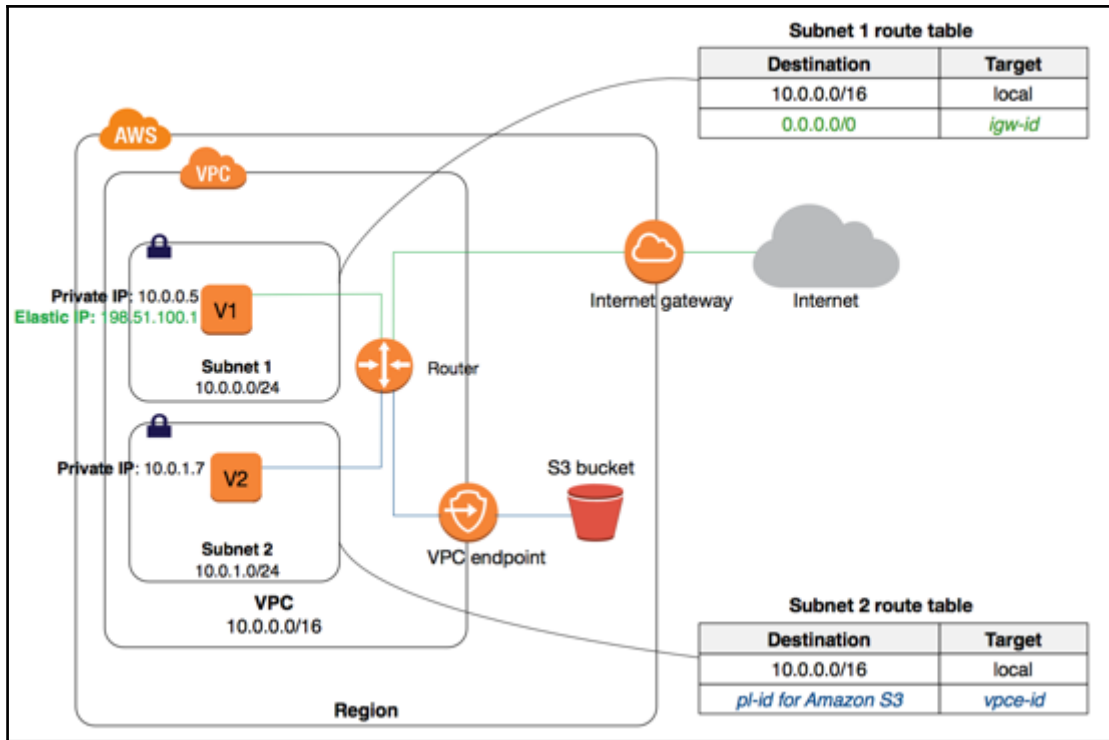
rtb-59331530

[Summary](#) [Routes](#) [Subnet Associations](#) [Route Propagation](#) [Tags](#)

[Edit](#)

View: All rules

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-a50e9ecc	Active	No



Services ▾ Resource Groups ▾ ☆

Step 1: Select a VPC Configuration

VPC with a Single Public Subnet

VPC with Public and Private Subnets

VPC with Public and Private Subnets and Hardware VPN Access

VPC with a Private Subnet Only and Hardware VPN Access

This configuration adds an IPsec Virtual Private Network (VPN) connection between your Amazon VPC and your data center - effectively extending your data center to the cloud while also providing direct access to the Internet for public subnet instances in your Amazon VPC.

Creates:

A /16 network with two /24 subnets. One subnet is directly connected to the Internet while the other subnet is connected to your corporate network via IPsec VPN tunnel. (VPN charges apply.)

[Select](#)

Internet, S3, DynamoDB, SNS, SQS, etc.

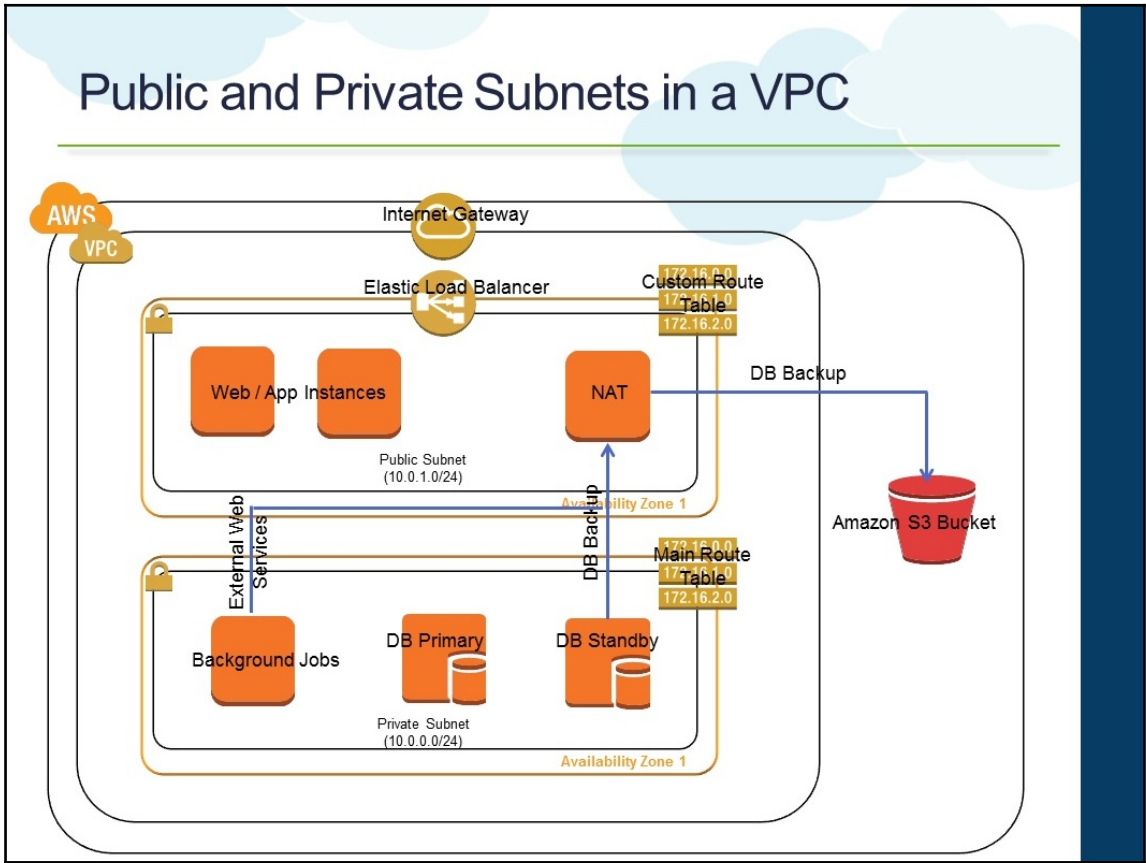
Amazon Virtual Private Cloud

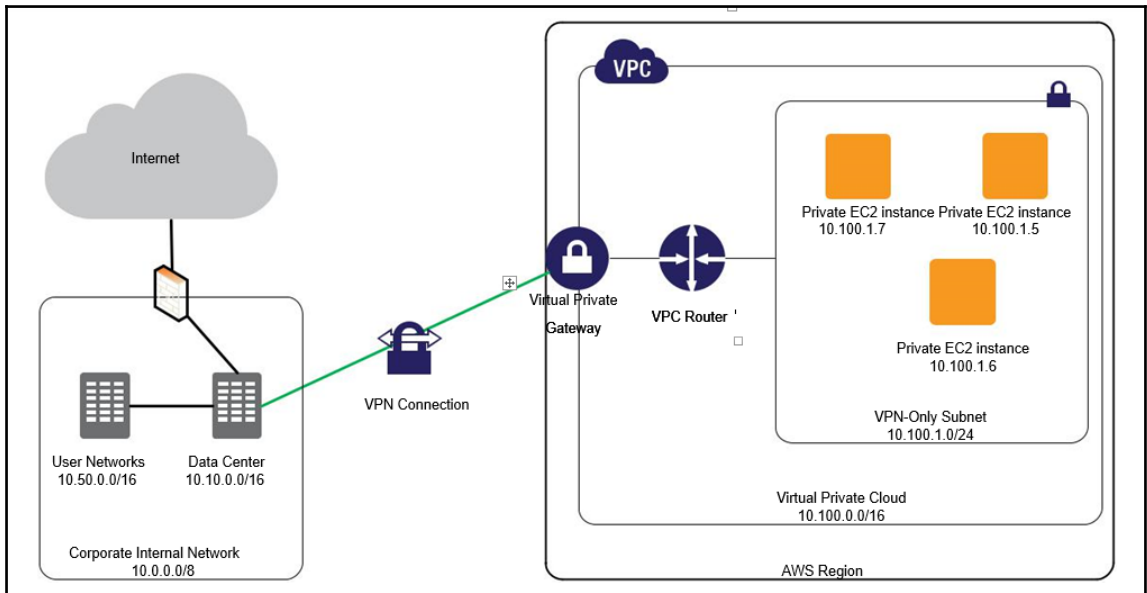
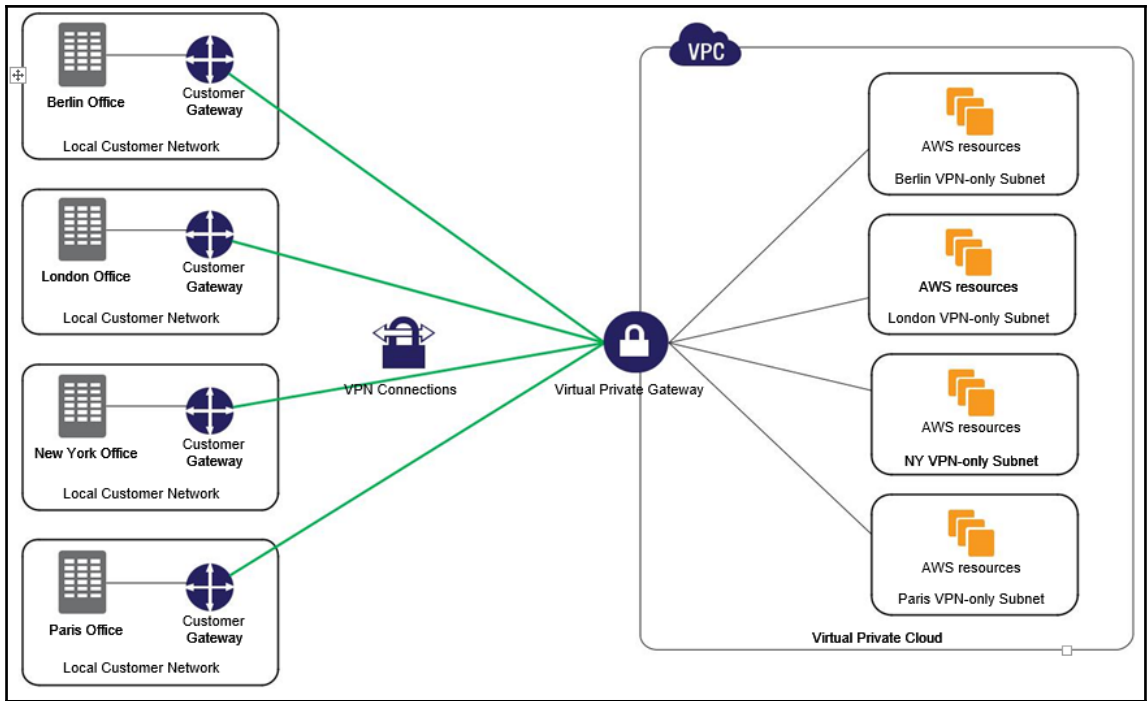
Public Subnet

Private Subnet

VPN

Corporate Data Center





Services ▾ Resource Groups ▾

Filter by VPC: None ▾

[Create Security Group](#) Security Group Actions ▾

Filter **All security groups** ▾

<input type="checkbox"/>	Name tag ▾	Group ID ▾	Group Name ▾	VPC ▾	Description
<input checked="" type="checkbox"/>	WebServer-SG	sg-9ce83cec	WebServer-SG	vpc-1f88c166 SL-VPC-Lab	Security Group for Web Servers
<input type="checkbox"/>	DBServer-SG	sg-0dee3a7d	DBServer-SG	vpc-1f88c166 SL-VPC-Lab	Database Server Security Group
<input type="checkbox"/>	Albert-SG	sg-631cc813	Albert-SG	vpc-1f88c166 SL-VPC-Lab	Albert-SG
<input type="checkbox"/>		sg-5337d422	default	vpc-ac13b4d5 My-SL-Lab-...	default VPC security group

sg-9ce83cec | WebServer-SG

Summary **Inbound Rules** Outbound Rules Tags

[Edit](#)

Type	Protocol	Port Range	Source
HTTP (80)	TCP (6)	80	0.0.0.0/0
SSH (22)	TCP (6)	22	0.0.0.0/0
HTTPS (443)	TCP (6)	443	0.0.0.0/0

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

NAT Gateways

Peering Connections

Security

Network ACLs

Security Groups

Services ▾ Resource Groups ▾

VPC Dashboard

Filter by VPC: None ▾

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

NAT Gateways

Peering Connections

Security

Network ACLs

Create Network ACL Delete

Search Network ACLs and the X

<input type="checkbox"/>	Name	Network ACL ID	Associated With	Default	VPC
<input checked="" type="checkbox"/>	SL-Public-NACL	acl-4bbf4133	1 Subnet	No	vpc-1f88c166 SL-VPC-Lab
<input type="checkbox"/>		acl-a65e78c0	6 Subnets	Yes	vpc-57fd6f31
<input type="checkbox"/>		acl-b86699c0	1 Subnet	Yes	vpc-1f88c166 SL-VPC-Lab

acl-4bbf4133 | SL-Public-NACL

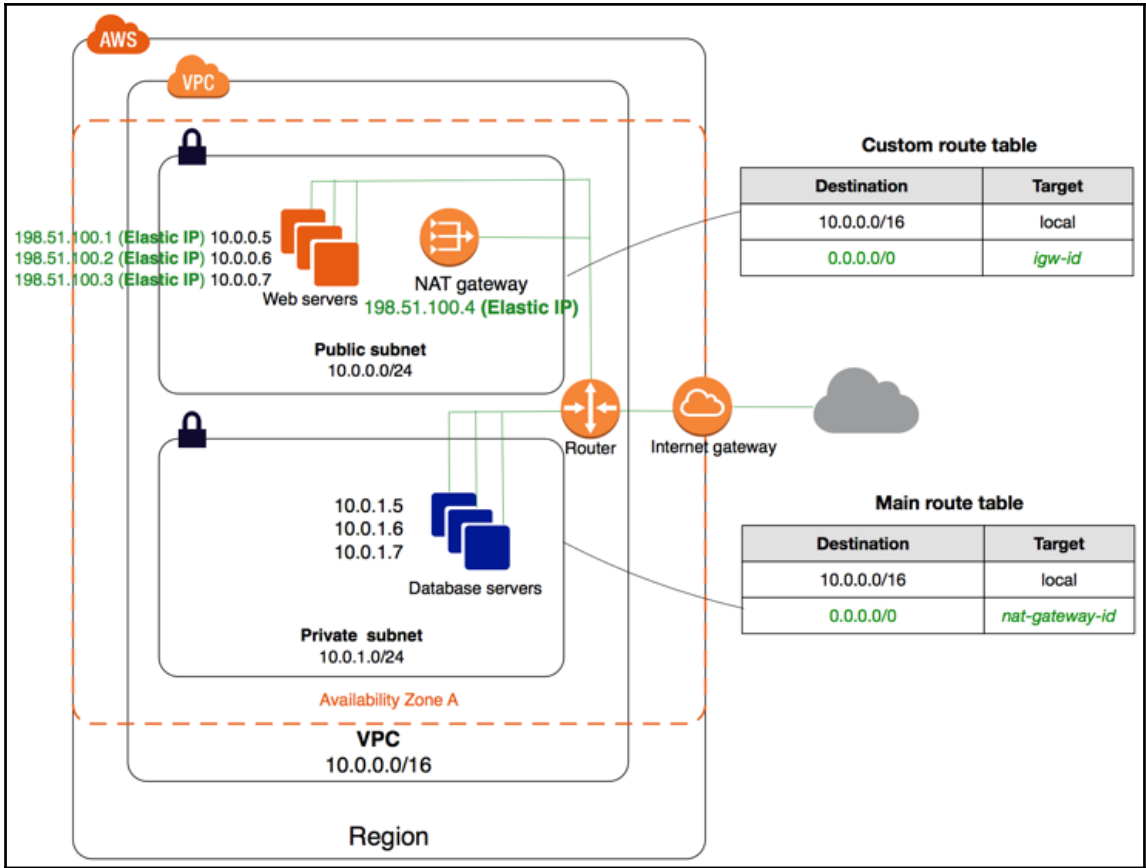
Summary **Inbound Rules** Outbound Rules Subnet Associations Tags

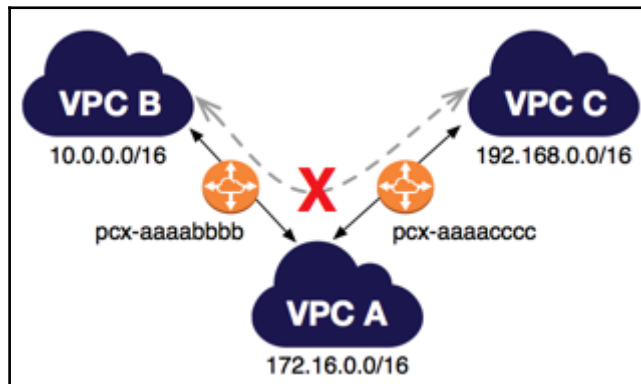
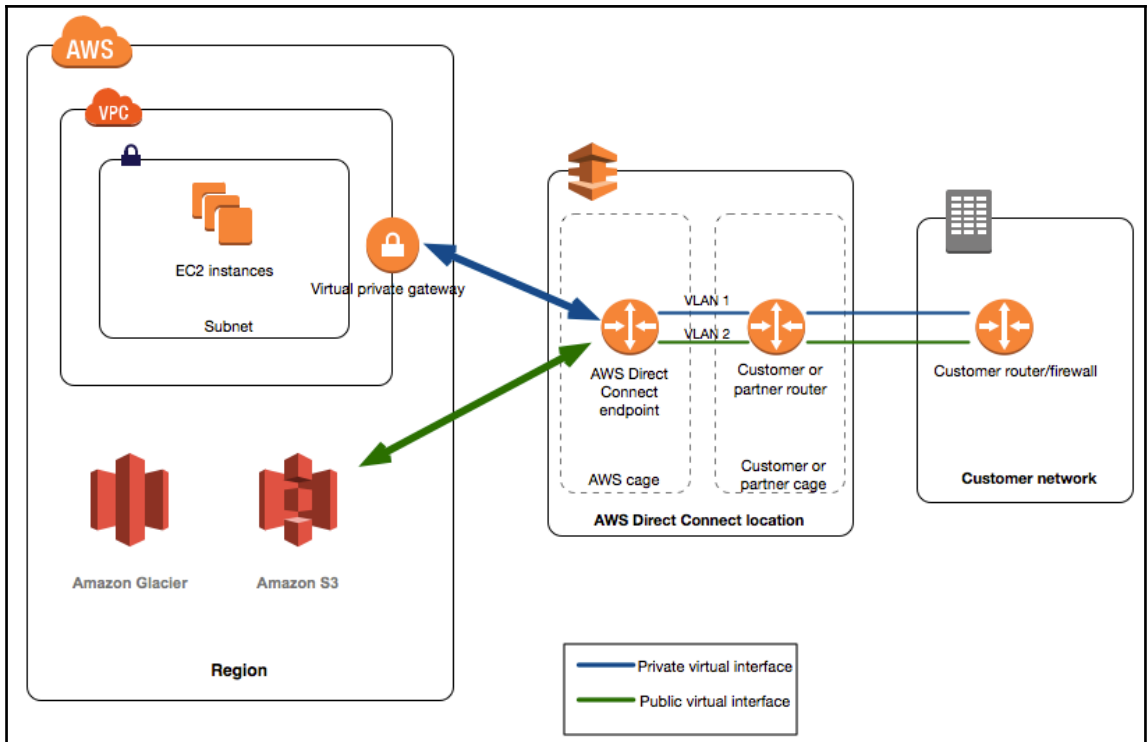
Allows inbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

Edit

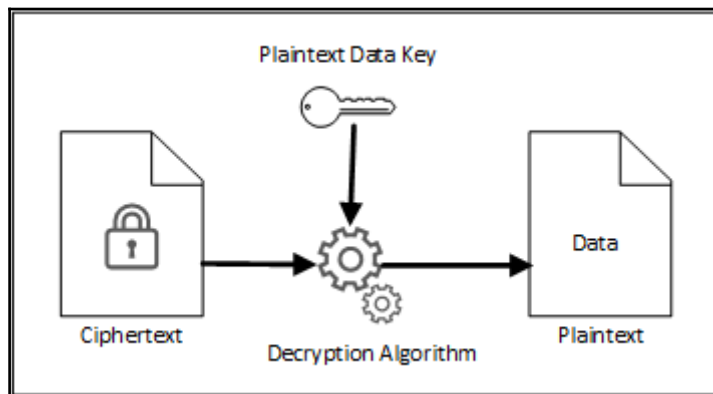
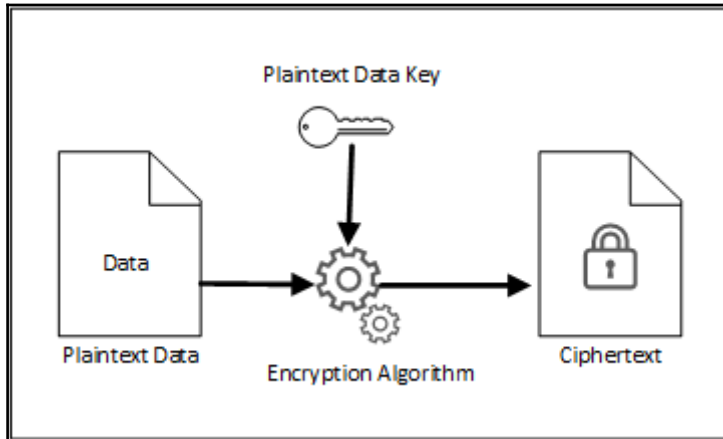
View: All rules ▾

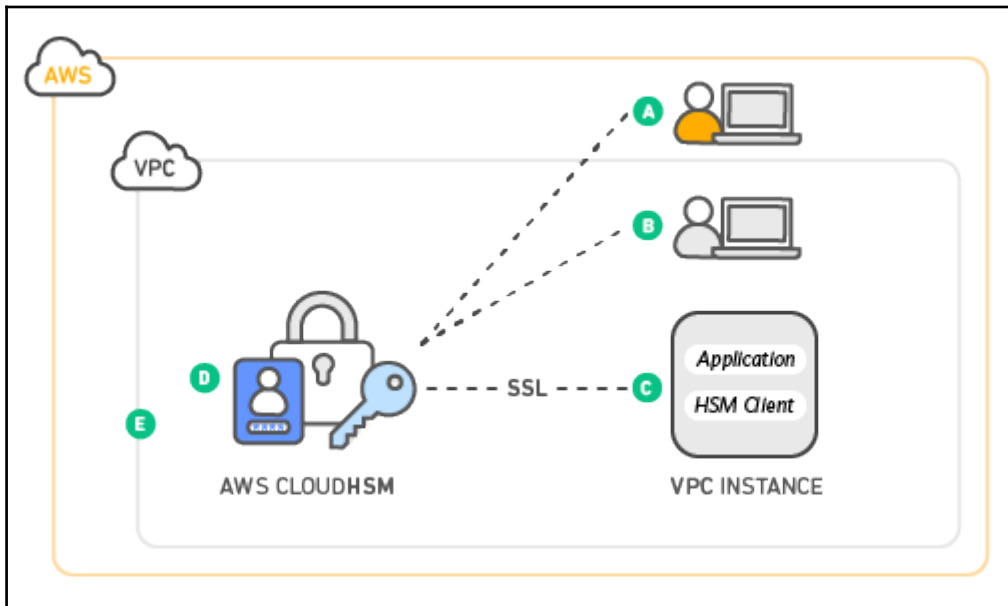
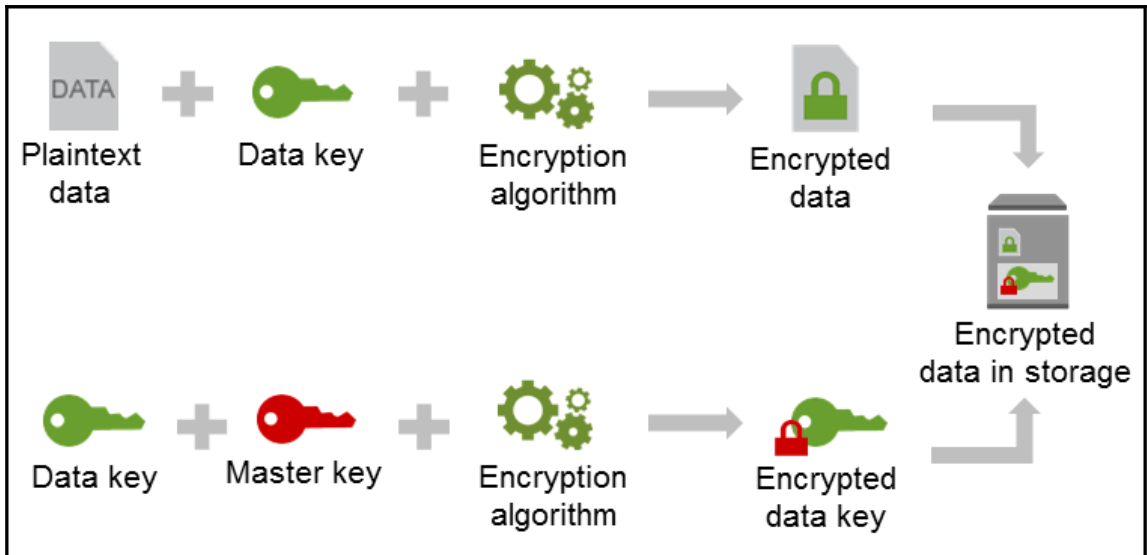
Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	HTTP (80)	TCP (6)	80	0.0.0.0/0	ALLOW
200	HTTPS (443)	TCP (6)	443	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

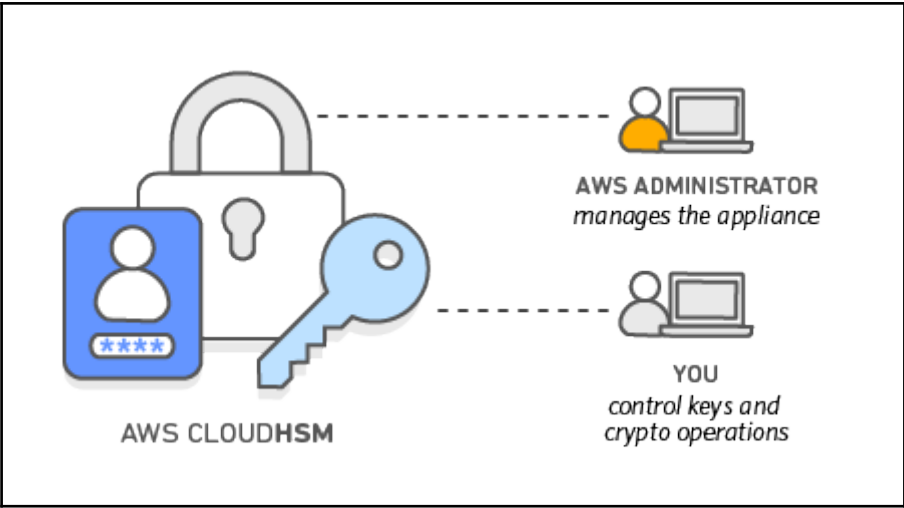




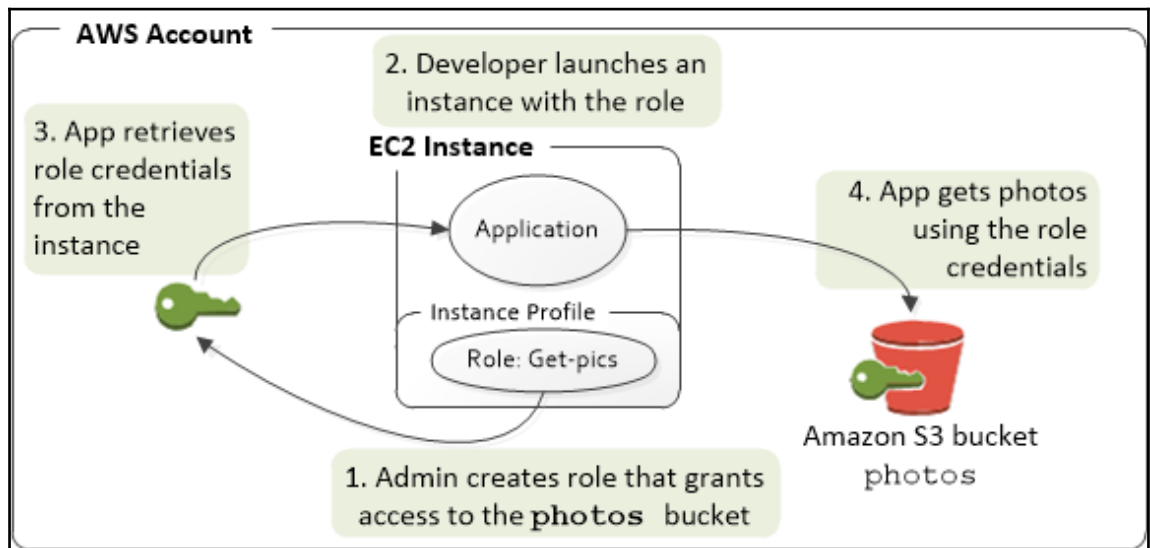
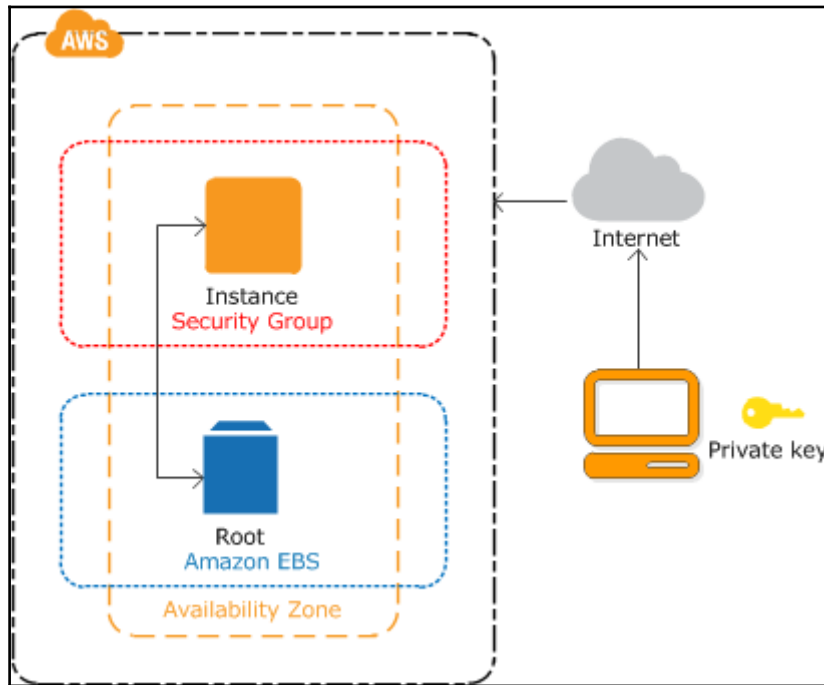
Chapter 4: Data Security in AWS







Chapter 5: Securing Servers in AWS



Services Resource Groups Albert N. Virginia Support

VPC Dashboard

Filter by VPC: Select a VPC

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

NAT Gateways

Peering Connections

Create Security Group Security Group Actions

Filter All security groups Search Security Groups and t X << 1 to 12 of 12 Security Groups >>

Name tag	Group ID	Group Name	VPC	Description
<input checked="" type="checkbox"/>	sg-36153c46	SL-Web-SG	vpc-571d6f31	Security group for Web Servers
<input type="checkbox"/>	sg-5940cf2a	Database Security Gr...	vpc-571d6f31	Database Servers Security Group

sg-36153c46 | Web Servers Security Group

Summary Inbound Rules Outbound Rules Tags

Cancel Save

Type	Protocol	Port Range	Source	Description	Remove
HTTP (80)	TCP (6)	80	0.0.0.0/0		
SSH (22)	TCP (6)	22	118.185.136.34/32		
HTTPS (443)	TCP (6)	443	0.0.0.0/0		

Add another rule

Services Resource Groups Albert N. Virginia Support

VPC Dashboard

Filter by VPC: Select a VPC

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

NAT Gateways

Peering Connections

Create Security Group Security Group Actions

Filter All security groups Search Security Groups and t X << 1 to 12 of 12 Security Groups >>

Name tag	Group ID	Group Name	VPC	Description
<input type="checkbox"/>	sg-36153c46	SL-Web-SG	vpc-4...	Security group for Web Servers
<input checked="" type="checkbox"/>	sg-5940cf2a	Database Security Gr...	vpc-4...	Database Servers Security Group
<input type="checkbox"/>	sg-21aaaf51	SecurityGroup-Allen	vpc-57...	Security Group created on 2017-...
<input type="checkbox"/>	sg-2e00055e	launch-wizard-1	vpc-57...	Security Group created on 2017-09-06T09:...

sg-5940cf2a | Database Security Group

Summary Inbound Rules Outbound Rules Tags

Cancel Save

Type	Protocol	Port Range	Source	Description	Remove
ALL Traffic	ALL	ALL	sg-21aaaf51		

Add another rule

sg-21aaaf51

sg-2e00055e

sg-36153c46 | Web Servers Security Group

sg-5705e024

sg-5940cf2a | Database Security Group

sg-700d0800

sg-7455c308

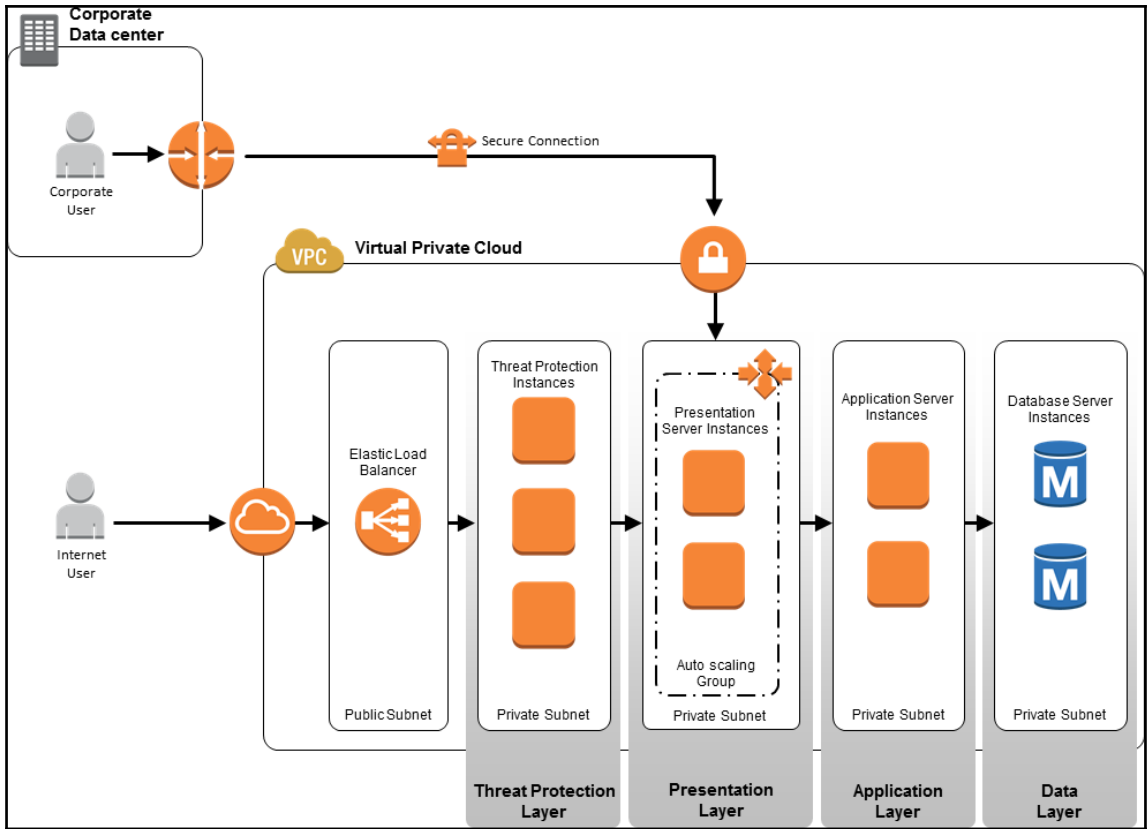
sg-8f0306ff

sg-920306e2

sg-e5090c95

sg-e70c0997

sg-e885659b




aws Services Resource Groups Albert Anthony N. Virginia


Amazon Inspector

Amazon Inspector enables you to analyze the behavior of your AWS resources and helps you identify potential security issues.


[Get started](#)



Install



Run



Analyze

aws Services Resource Groups Albert N. Virginia Support

[Create a trail](#)
You can create a trail to retain a record of your CloudTrail events. With a trail, you can also create event metrics, trigger alerts, and create event workflows. [Learn more](#) [Create trail](#)

Event history

Your event history contains the create, modify, and delete activities for supported services taken by people, groups, or AWS services in your AWS account. To view a complete log of your CloudTrail events, create a trail and then go to your Amazon S3 bucket or CloudWatch Logs.

You can view the last 7 days of events. Choose an event to view more information about it. [Learn more](#)

Filter: **Event source** inspector.amazonaws.com Time range: Select time range

Event time	User name	Event name	Resource type	Resource name
▶ 2017-09-23, 07:09:52...	root	StartAssessmentRun		
▶ 2017-09-23, 08:13:54...	root	CreateAssessmentTe...		
▶ 2017-09-23, 08:13:53...	root	CreateAssessmentTa...		
▶ 2017-09-23, 08:13:52...	root	CreateResourceGroup		
▶ 2017-09-23, 07:56:42...	root	RegisterCrossAccou...		
▶ 2017-09-23, 07:56:39...	root	RegisterCrossAccou...		

aws Services Resource Groups

Albert N. Virginia Support

CloudWatch Dashboards

Alarms

ALARM

INSUFFICIENT

OK

Billing

Events

Rules

Event Buses ^{NEW}

Logs

Metrics

Amazon Inspector 1h 3h 12h 1d 3d 1w custom Line Actions

All metrics Graphed metrics (4) Graph options

All > Inspector > Metrics by Target Search for any metric, dimension or resource id

<input checked="" type="checkbox"/>	AssessmentTargetName (4)	AssessmentTargetArn	Metric Name
<input checked="" type="checkbox"/>	Web-Server	arn:aws:inspector:us-east-1:100122829558	TotalAssessmentRuns
<input checked="" type="checkbox"/>	Web-Server	arn:aws:inspector:us-east-1:100122829558	TotalMatchingAgents
<input checked="" type="checkbox"/>	Web-Server	arn:aws:inspector:us-east-1:100122829558	TotalHealthyAgents
<input checked="" type="checkbox"/>	Web-Server	arn:aws:inspector:us-east-1:100122829558	TotalFindings

aws Services Resource Groups

Albert N. Virginia Support

Dashboard

Assessment targets

Assessment templates

Assessment runs

Findings

Amazon Inspector ?

Amazon Inspector enables you to analyze the behavior of your AWS resources and helps you identify potential security issues. [Learn more.](#)

Notable findings

- 0 Important findings
- 1 Recent finding

Assessment status

- 0 Assessments running
- 1 Assessment runs completed
- 0 Assessment runs failed

Account settings

[Manage Amazon Inspector service role](#)

Recent Assessment Runs (Last 10)

Name	Date Run	Status
Run - WebServer - 2017-09-23T13:39:50.208Z	Today at 7:09 PM (GMT+5)	Analysis complete

aws Services Resource Groups

Albert N. Virginia Support

Get started with Amazon Inspector

Step 1: Prerequisites
Step 2: Define an assessment target
Step 3: Define an assessment template
Step 4: Review

Define an assessment template

An assessment template allows you to specify various properties for an assessment run, including rules packages, duration, SNS notifications, and how to label any findings. [Learn more.](#)

Name* WebServer

Rules packages* Select an Inspector rules package

Duration* Runtime Behavior Analysis-1.0

*Required

Cancel Previous Next

Name	Duration	Target name	Last run	All runs
Web Servers	na	Web-Server		

Assessment Template - Web Servers

Name* Web Servers

Target name* Web-Server

Rules packages* Security Best Practices-1.0

Duration* 1 hour (Recommended)

Key	Value
Add a new key	

Key	Value
Add a new key	Add a new value

AWS Shield

Standard Protection






*Available to ALL AWS customers at
No Additional Cost*

Advanced Protection



*Paid service that provides additional,
comprehensive protections from large
and sophisticated attacks*

Chapter 6: Securing Applications in AWS

 <p>Web traffic filtering with custom rules</p> <p>Create custom rules that can allow, block, or count web requests based on originating IP addresses or strings that appear</p>	 <p>Block malicious requests</p> <p>Configure AWS WAF to recognize and block common web application security risks like SQL injection (SQLi) and cross-site scripting (XSS).</p>	 <p>Tune your rules and monitor traffic</p> <p>Review details about the web requests that AWS WAF allows, blocks, or counts, and update rules to thwart new attacks.</p>
--	--	--

IP match condition example
Suspicious IPs
192.0.2.0/24
192.51.100.0/24
2001:db8:a0b:12f0:ac34:1:1:1/128
2001:db8:a0b:12f0:0:0:0:0/64

Rules example

Bad User-Agents

IP match condition

Suspicious IPs

and

String match condition

Bad bots



Web ACL

- Combines rules with an OR
- Checks rules in order listed
 - Specifies action if rule is met
 - Specifies default action if no rule is met

Rate-based rule
(combines conditions with an AND and adds a rate limit)



Condition
Example: Cross-site scripting threat

AND



Condition
Example: Specific IP addresses

AND



Rate limit: 15,000

If rule is met: do this action (Example: block)

Rule
(combines conditions with an AND)



Condition
Example: SQL injection threat

AND

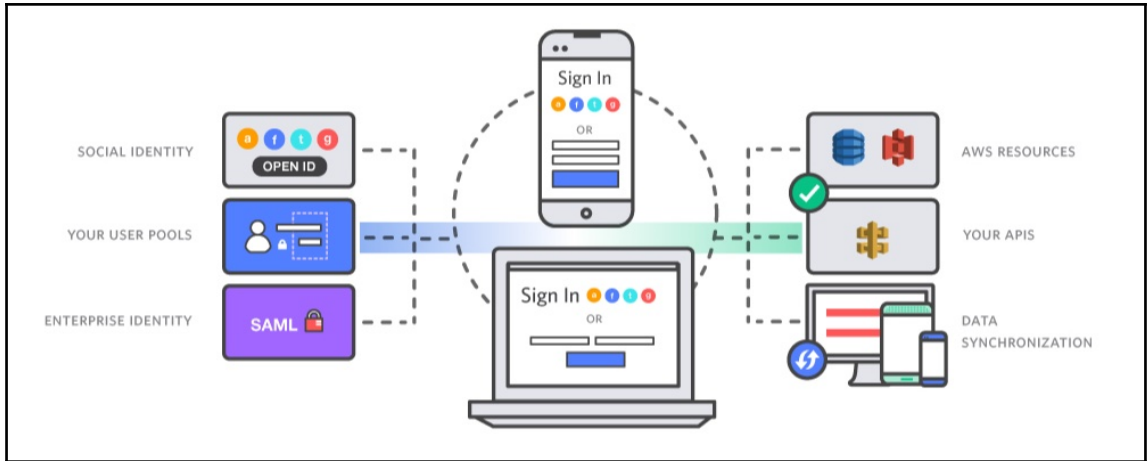


Condition
Example: Specific string in header

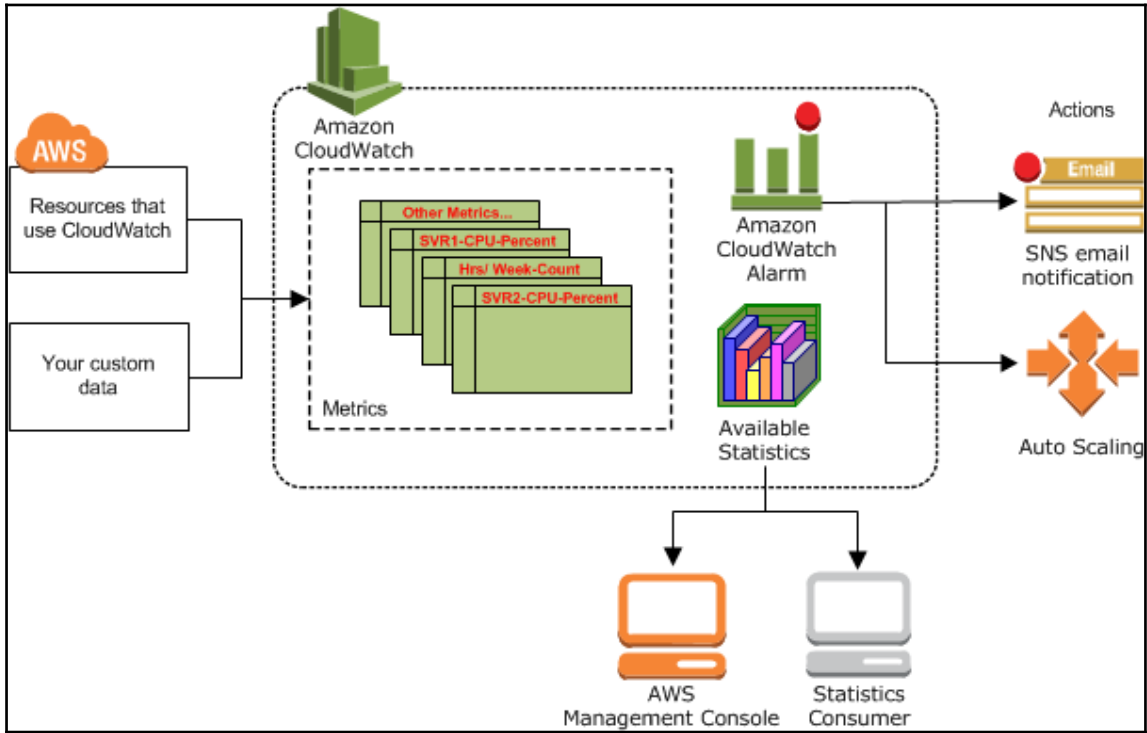
OR

If rule is met: do this action (Example: count)

If no rules match, perform default action (Example: allow)



Chapter 7: Monitoring in AWS



aws
CloudWatch Dashboards
Alarms

1. [Select Metric](#) 2. **Define Alarm**

Alarm Threshold

Provide the details and threshold for your alarm. Use the graph on the right to help set the appropriate threshold.

Name:

Description:

Whenever charges for: **is:**

Additional settings

Provide additional configuration for your alarm.

Treat missing data as:

Alarm Preview

This alarm will trigger when the blue line goes up to or above the red line

Namespace: AWS/Billing

Currency:

Metric Name:

Cancel
Previous
Next
Create Alarm

aws
Services
Resource Groups
Albert Anthony
N. Virginia
Support

CloudWatch

Dashboards

WordPress-Dashboard

Alarms

ALARM

INSUFFICIENT

OK

Billing

Events

Rules

Event Buses NEW

Logs

Metrics

WordPress-Dashboard
Add widget
Actions
Save dashboard

CPUUtilization

VolumeReadOps, Volu...

Latency, RequestCount

S3 Object Count

EstimatedCharges

1h 3h 12h 1d 3d 1w custom (15mo)

All metrics Graphed metrics (13) Graph options

Search for any metric, dimension or resource id

338 Metrics


Billing 14 Metrics	DynamoDB 14 Metrics	EBS 81 Metrics
EC2 136 Metrics	RDS 72 Metrics	S3 8 Metrics
SNS 4 Metrics	SQS 9 Metrics	

All metrics Graphed metrics (9) Graph options


Label	Namespace	Dimensions	Metric Name	Statistic	Period	Y Axis	Actions
AmazonCloudWatch	AWS/Billing	Dimensions (2)	EstimatedCharges	Maximum	6 Hours	< >	
AmazonEC2	AWS/Billing	Dimensions (2)	EstimatedCharges	Maximum	6 Hours	< >	
AmazonRDS	AWS/Billing	Dimensions (2)	EstimatedCharges	Maximum	6 Hours	< >	
AmazonS3	AWS/Billing	Dimensions (2)	EstimatedCharges	Maximum	6 Hours	< >	
AmazonSNS	AWS/Billing	Dimensions (2)	EstimatedCharges	Maximum	6 Hours	< >	
AWSDataTransfer	AWS/Billing	Dimensions (2)	EstimatedCharges	Maximum	6 Hours	< >	
awskms	AWS/Billing	Dimensions (2)	EstimatedCharges	Maximum	6 Hours	< >	

Add to this dashboard ✕


Select a widget type to configure and add to this dashboard.




Line
Compare metrics over time



Stacked area
Compare the total over time




Number
Instantly see the latest value for a metric



Text
Free text with markdown formatting

[Cancel](#) [Configure](#)

Start Responding to CloudWatch Events



Determine events of interest in the CloudWatch Events stream

Create rules to select events of interest

Specify actions to take when a rule matches an event

Create Alarm

1. **Select Metric** 2. Define Alarm

EC2 1 to 50 of 68 Metrics

Per-Instance Metrics By Auto Scaling Group By Image (AMI) Id Aggregated by Instance Type Across All Instances

EC2 > Per-Instance Metrics

<input type="checkbox"/>	InstanceId	InstanceName	Metric Name
<input type="checkbox"/>	i-0332c3c79f97a3e63		CPUCreditBalance
<input type="checkbox"/>	i-0332c3c79f97a3e63		CPUCreditUsage
<input checked="" type="checkbox"/>	i-0332c3c79f97a3e63		CPUUtilization
<input type="checkbox"/>	i-0332c3c79f97a3e63		DiskReadBytes
<input type="checkbox"/>	i-0332c3c79f97a3e63		DiskReadOps

Title: CPUUtilization Average 5 Minutes Update Graph

Time Range: Relative Absolute UTC (GMT)

From: 3 days ago To: 0 hours ago

Zoom: 1h | 3h | 6h | 12h | 1d | 3d | 1w | 2w

Left Y-axis: Limits Min 0 Max Auto Auto

Cancel Previous **Next** Create Alarm

LambdaLog

1h 3h 12h 1d 3d 1w custom Stacked area Actions

View logs in this time range

AWS/Logs - /aws/lambda/S3LambdaPutFunction

Add to dashboard Share

View logs

All metrics Graphed metrics (2) Graph options

All > Logs > Log Group Metrics

<input checked="" type="checkbox"/>	LogGroupName (2)	Metric Name
<input checked="" type="checkbox"/>	/aws/lambda/S3LambdaPutFunction	IncomingLogEvents
<input checked="" type="checkbox"/>	/aws/lambda/S3LambdaPutFunction	IncomingBytes

Define Logs Metric Filter

Filter for Log Group: /aws/lambda/S3LambdaPutFunction

You can use metric filters to monitor events in a log group as they are sent to CloudWatch Logs. You can monitor and count specific terms or extract values from log events and associate the results with a metric. [Learn more about pattern syntax.](#)

Filter Pattern

[Show examples](#)

Select Log Data to Test

Test Pattern

Clear

Loading function

START RequestId: 3d2a2042-689b-11e7-ac85-158ea65b4e01 Version: \$LATEST

An error occurred (AccessDenied) when calling the GetObject operation: Access Denied

Results

Please paste logs lines above and click **Test Pattern**.

Cancel

Assign Metric

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
wordpress in...	i-0a8b6f46708f94aaf	t2.micro	ap-south-1a	running	2/2 checks passed	None	ec2-13-126-201-229.ap...
Test Wordpr...	i-0bdeb80221ef3d07	t2.micro	ap-south-1a	running	2/2 checks passed	None	ec2-52-66-170-35.ap-s...

Instance: **i-0bdeb80221ef3d07 (Test Wordpress Instance)** Public DNS: ec2-52-66-170-35.ap-south-1.compute.amazonaws.com

Status Checks Monitoring Tags Usage Instructions

Status checks detect problems that may impair this instance from running your applications. [Learn more](#) about status checks.

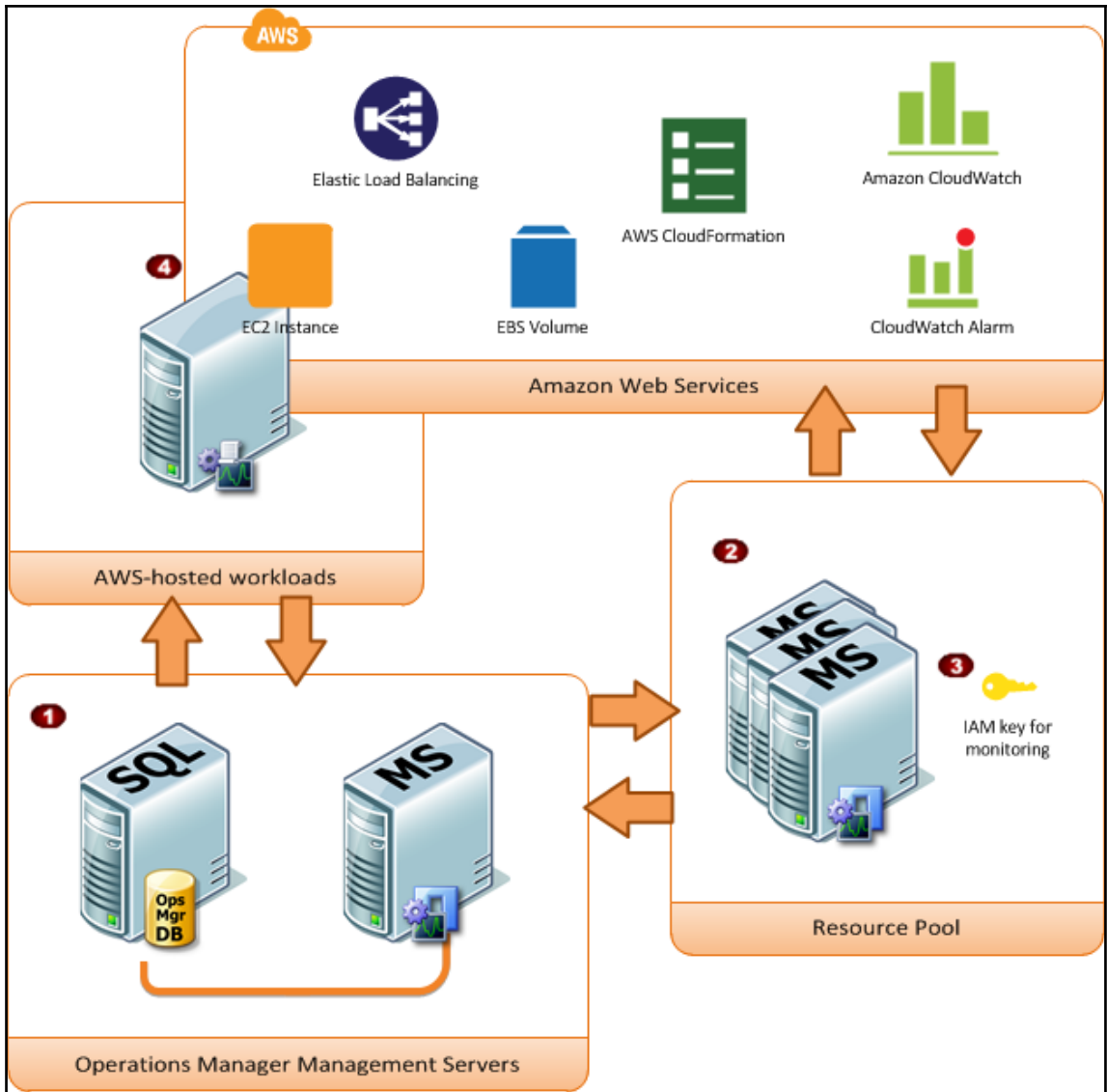
Create Status Check Alarm

System Status Checks **Instance Status Checks**

These checks monitor the AWS systems required to use this instance and ensure they are functioning properly.
System reachability check passed

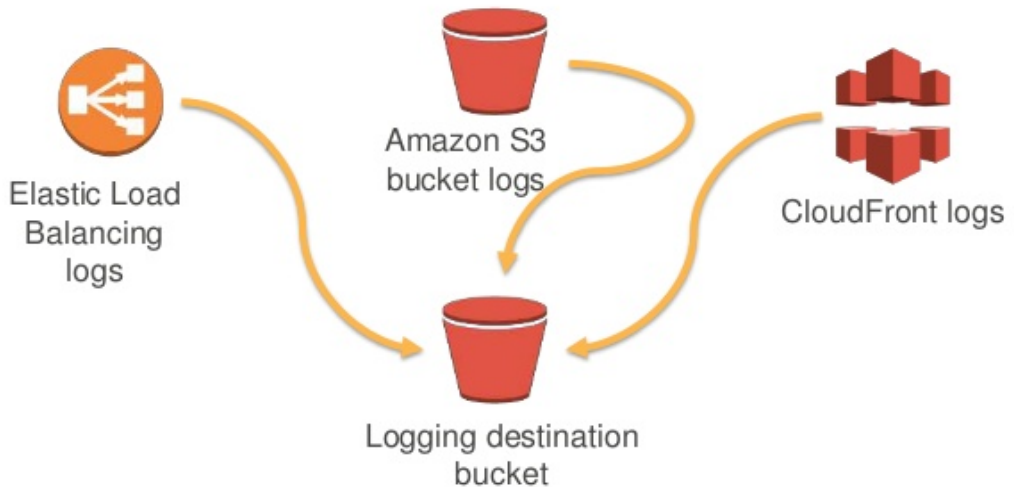
These checks monitor your software and network configuration for this instance.
Instance reachability check passed

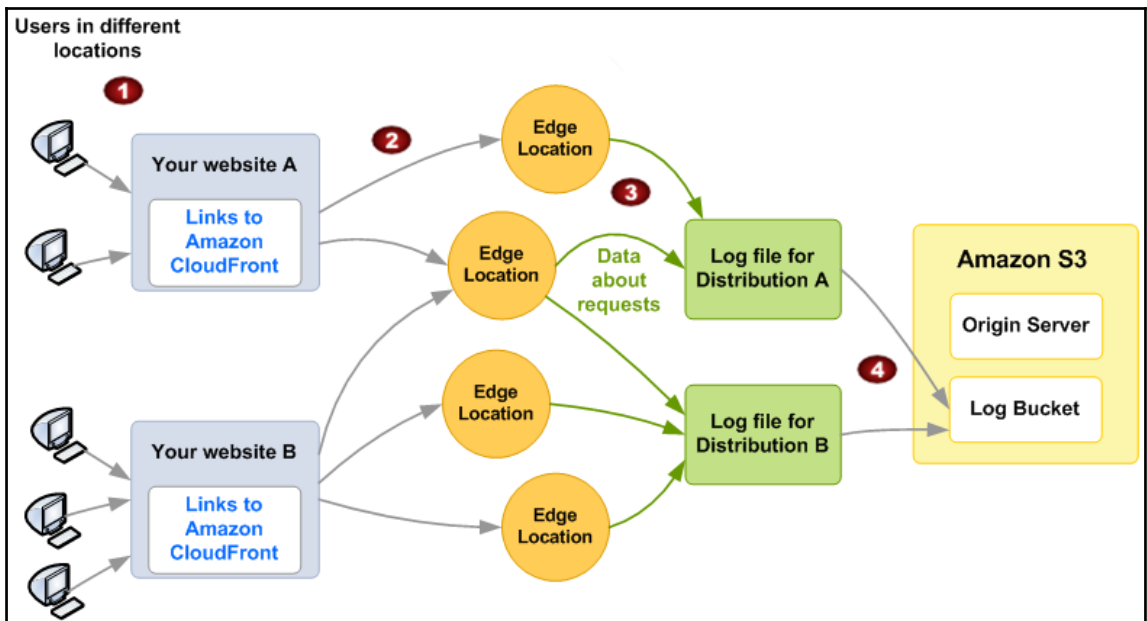
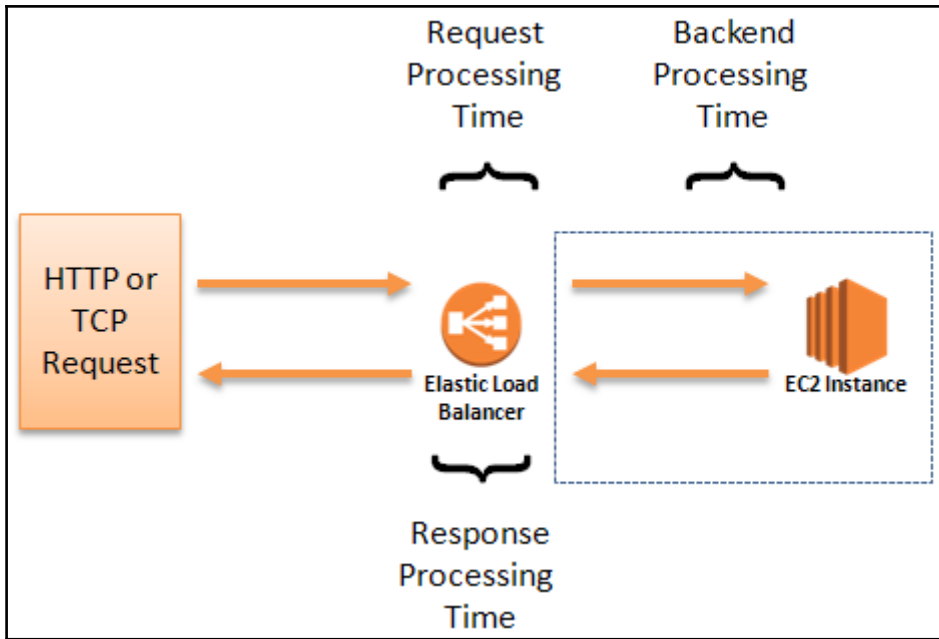
This check verifies that your instance's operating system is accepting traffic. If this check fails, you may need to reboot your instance or make modifications to your operating system configuration.



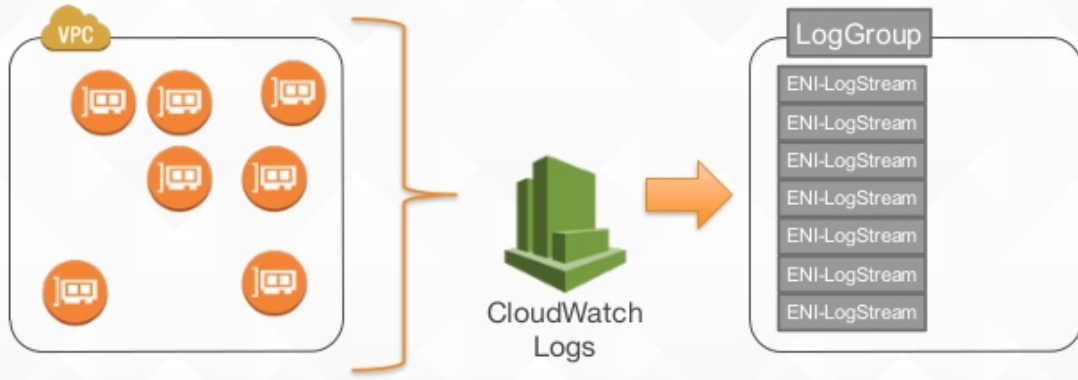
Chapter 8: Logging and Auditing in AWS

Logging—Elastic Load Balancing, CloudFront, Amazon S3 access logs





VPC Flow Logs



CloudWatch > Log Groups

Create Metric Filter Actions ▾

Filter: Log Group Name Prefix x << < Log Groups 1-4

Log Groups	Expire Events After	Metric Filters	Subscriptions
<input checked="" type="radio"/> /aws/lambda/S3LambdaPutFunction	Never Expire	2 filters	None
<input type="radio"/> /aws/lambda/SNSLambdaFunction	Never Expire	0 filters	None
<input type="radio"/> /aws/lambda/myFunction	Never Expire	0 filters	None
<input type="radio"/> /aws/lambda/myfunction	Never Expire	0 filters	None

CloudWatch > Log Groups > Streams for /aws/lambda/S3LambdaPutFunction

Search Log Group Create Log Stream Delete Log Stream

Filter: Log Stream Name Prefix x << < Log Streams 1-50 >

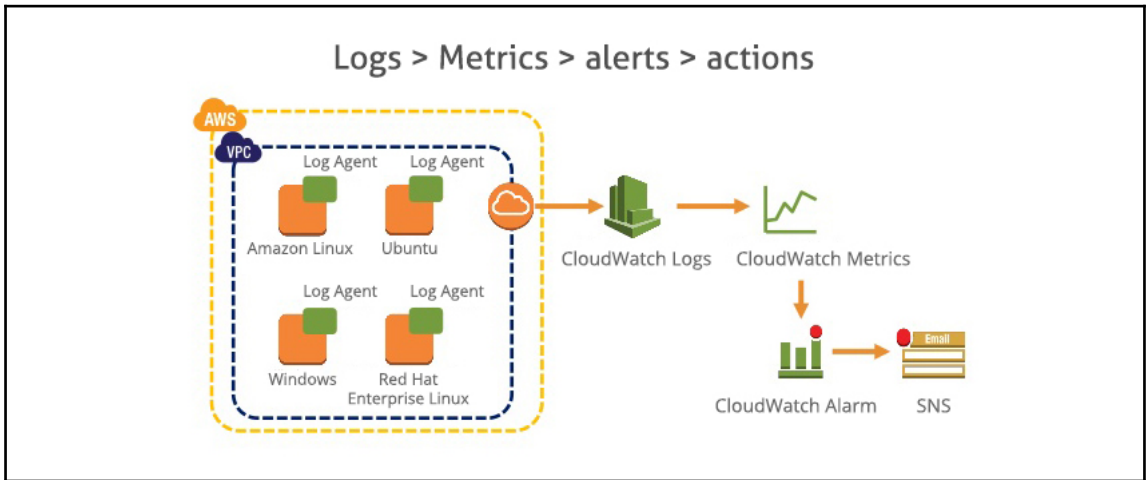
Log Streams	Last Event Time
<input type="checkbox"/> 2017/10/07/[\$LATEST]e03d91ab00d84158b3f7e423c0396b7a	2017-10-07 21:30 UTC+5:30
<input type="checkbox"/> 2017/10/07/[\$LATEST]6a945f8450c44ab2877b3731293f9060	2017-10-07 21:23 UTC+5:30
<input type="checkbox"/> 2017/10/07/[\$LATEST]93e60de3239f45ceb0b6b939c77610f9	2017-10-07 21:20 UTC+5:30
<input type="checkbox"/> 2017/10/07/[\$LATEST]8047709d14504d0f8511e2f37d9438b7	2017-10-07 20:11 UTC+5:30
<input type="checkbox"/> 2017/10/07/[\$LATEST]a8b8b02652bb444aabf83dbf0936acc4	2017-10-07 20:07 UTC+5:30

CloudWatch > Log Groups > /aws/lambda/S3LambdaPutFunction > 2017/10/07/[\$LATEST]6a945f8450c44ab2877b3731293f9060

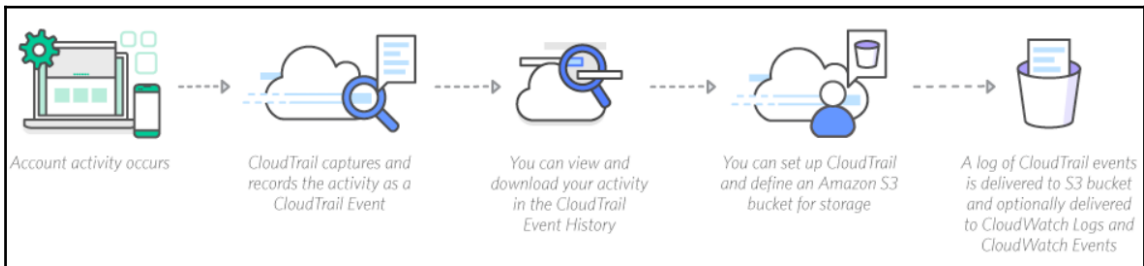
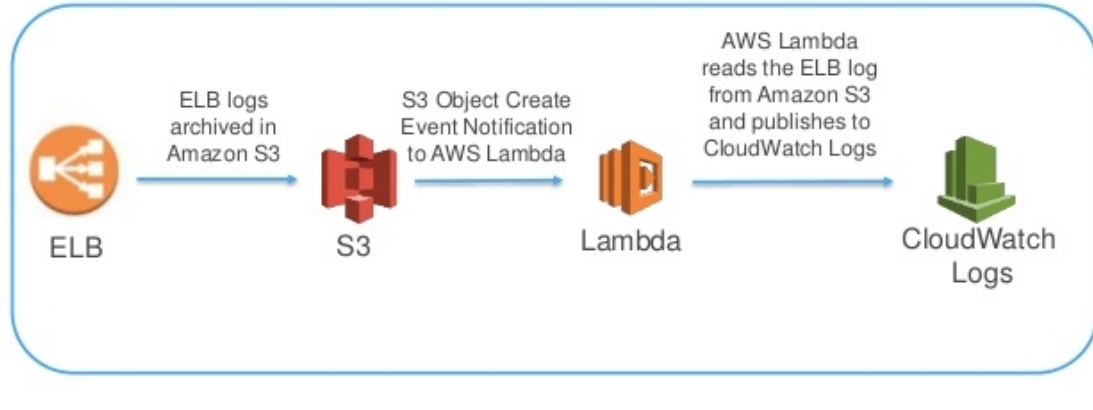
Expand all Row Text

Filter events 30s 5m 1h 6h 1d 1w custom ▾

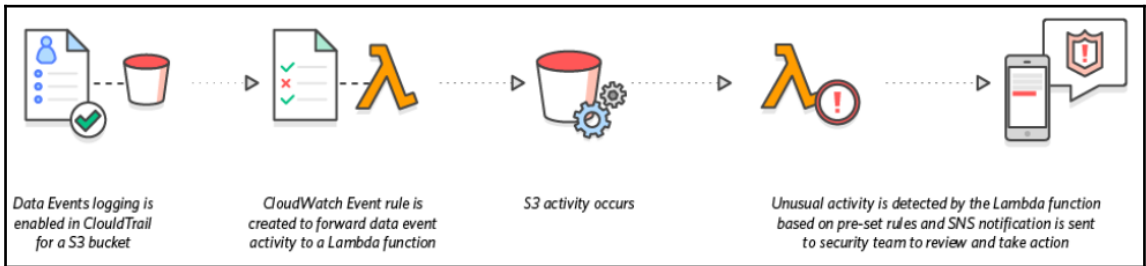
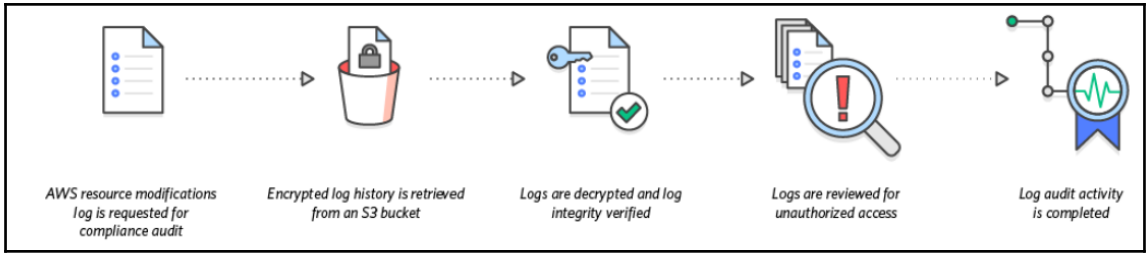
Time (UTC +00:00)	Message
2017-10-07	
An error occurred (AccessDenied) when calling the GetObject operation: Access Denied	
15:53:06	Error getting object AWSLogs/902891488394/CloudTrail/us-east-2/2017/10/07/902891488394_CloudTrail_us-east-2_20171007T1545Z
Error getting object AWSLogs/902891488394/CloudTrail/us-east-2/2017/10/07/902891488394_CloudTrail_us-east-2_20171007T1545Z_w0nojt86lRmmnx5N.json.gz from bucket albertanthony. Make sure they exist and your bucket is in the same region as this function.	
15:53:06	An error occurred (AccessDenied) when calling the GetObject operation: Access Denied: ClientError Traceback (most recent call last):
15:53:06	END RequestId: 9bb64113-ab77-11e7-854b-cd5426b48afd
15:53:06	REPORT RequestId: 9bb64113-ab77-11e7-854b-cd5426b48afd Duration: 21.48 ms Billed Duration: 100 ms Memory Size: 128 MB Max
15:53:06	START RequestId: 791ea986-ab77-11e7-85b3-bfe3ee4a8df1 Version: \$LATEST
15:53:06	An error occurred (AccessDenied) when calling the GetObject operation: Access Denied
15:53:06	Error getting object AWSLogs/902891488394/CloudTrail/ap-northeast-1/2017/10/07/902891488394_CloudTrail_ap-northeast-1_20171007T1545Z



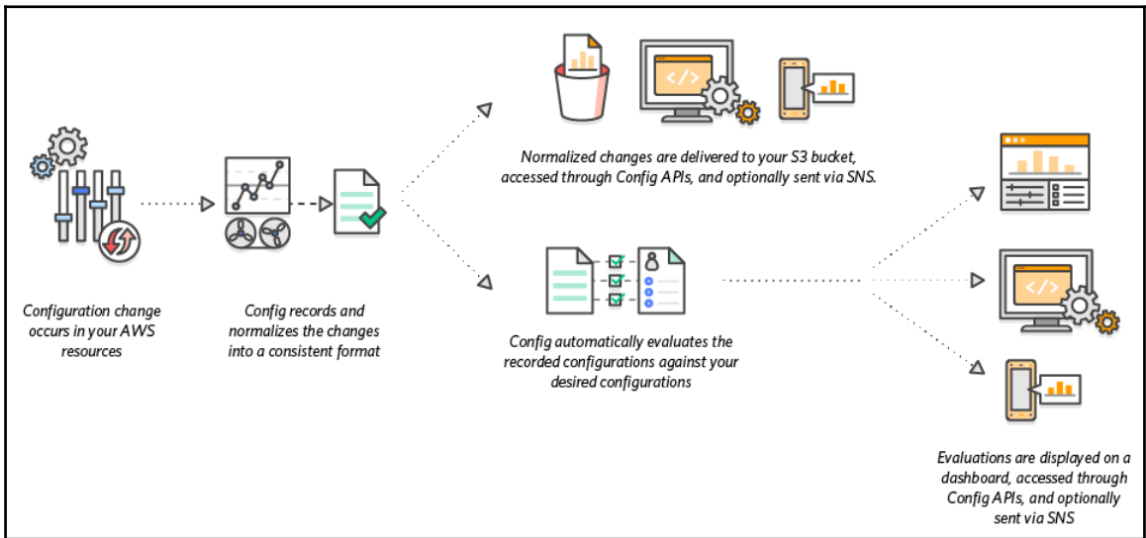
Flow of events

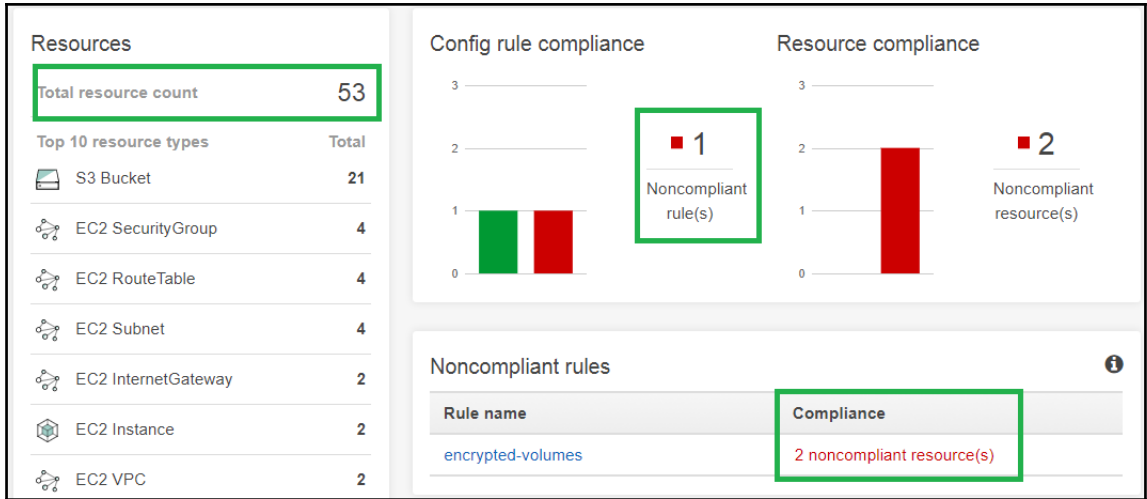



Event time	User name	Event name	Resource type
▶ 2017-10-08, 08:56:01 ...	root	ConsoleLogin	
▼ 2017-10-08, 04:31:42 ...	S3LambdaPutFunction	CreateLogStream	
AWS access key ASIAJRGSLRIJL2TUS5SQ		Event source logs.amazonaws.com	
AWS region ap-south-1		Event time 2017-10-08, 04:31:42 PM	
Error code		Request ID 11232d98-ac18-11e7-bdb0-d356217574b0	
Event ID 9c7d0d4e-cfb5-4bac-b5bb-6b108f6720a8		Source IP address 52.66.68.156	
Event name CreateLogStream		User name S3LambdaPutFunction	
Resources Referenced (0)			




Key AWS Certifications and Assurance Programs








Create and manage portfolios
Use portfolios to organize your products and distribute them to end users.

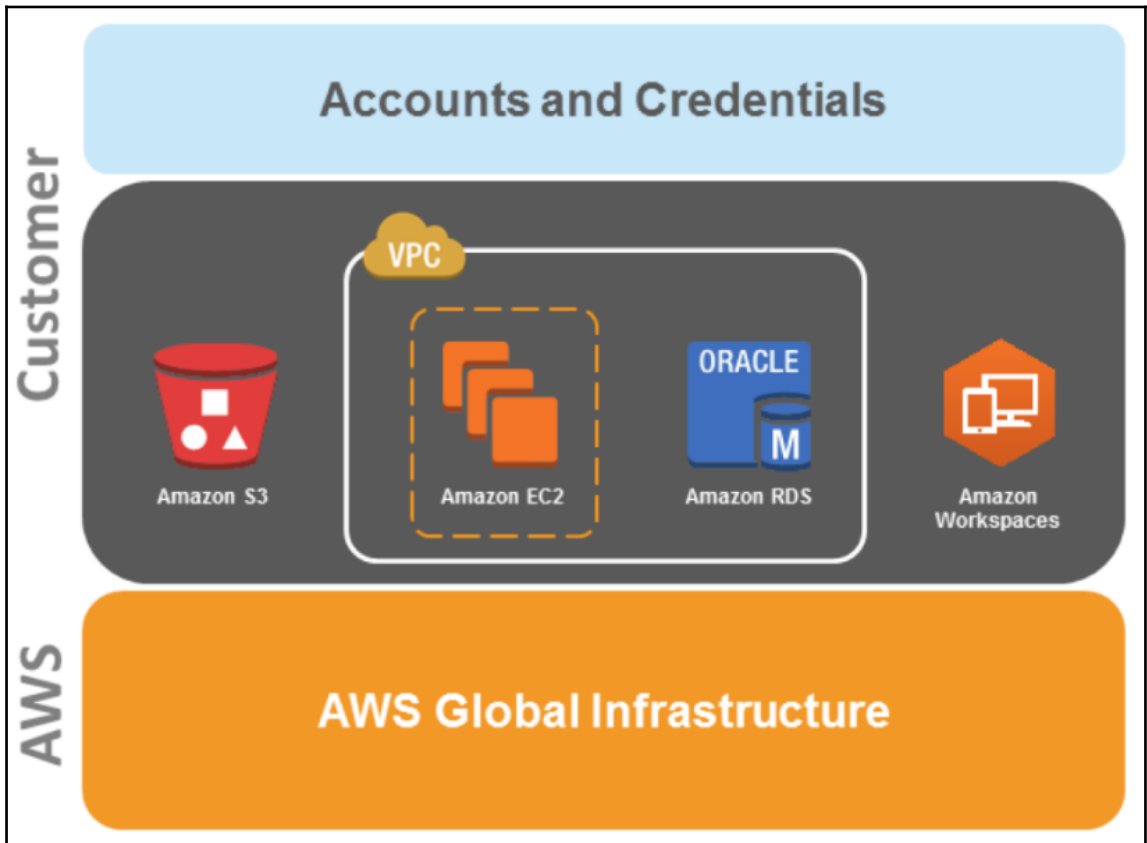


Add products
You can upload your line of business products or products you already own licenses to.



Manage user access
Decide who can access products and set policies on where and how users can launch them.

Chapter 9: AWS Security Best Practices



Security Status

5 out of 5 complete.

- Delete your root access keys ▼
- Activate MFA on your root account ▼
- Create individual IAM users ▼
- Use groups to assign permissions ▼
- Apply an IAM password policy ▼



BUSINESS



PLATFORM



PEOPLE



SECURITY



GOVERNANCE



OPERATIONS

Table of Contents

Index

2

Index